DZIAŁ ZAMÓWIEŃ PUBLICZNYCH
UNIWERSYTETU JAGIELLOŃSKIEGO
ul. Straszewskiego 25/3 i 4, 31-113 Kraków
tel. +4812-663-39-03
e-mail: bzp@uj.edu.pl
https://www.uj.edu.pl ; https://przetargi.uj.edu.pl

Kraków, dnia 12.07.2024 r.

SPECYFIKACJA WARUNKÓW ZAMÓWIENIA
zwana dalej w skrócie SWZ

Rozdział I - Nazwa (firma) oraz adres Zamawiającego.

1. Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków.
2. Jednostka prowadząca sprawę:
   2.1 Dział Zamówień Publicznych, ul. Straszewskiego 25/3 i 4, 31-113 Kraków; tel.: +4812 663-39-03;
   2.2 godziny urzędowania: od poniedziałku do piątku; od 7:30 do 15:30, z wyłączeniem sobót oraz dni ustawowo wolnych od pracy;
   2.3 strona internetowa (adres url): https://www.uj.edu.pl/
   2.4 narzędzie komercyjne do prowadzenia postępowania: https://platformazakupowa.pl
   2.5 adres strony internetowej prowadzonego postępowania, na której udostępniane będą zmiany i wyjaśnienia treści SWZ oraz inne dokumenty zamówienia bezpośrednio związane z postępowaniem (adres profilu nabywcy – narzędzie komercyjne): https://platformazakupowa.pl/transakcja/954255

Rozdział II - Tryb udzielenia zamówienia.

1. Postępowanie prowadzone jest w trybie podstawowym bez możliwości negocjacji na podstawie art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t. j. Dz. U. 2023 poz. 1605 ze zm.), zwanej dalej ustawą PZP, oraz zgodnie z wymogami określonymi w niniejszej Specyfikacji Warunków Zamówienia, zwanej dalej „SWZ".
2. Do czynności podejmowanych przez Zamawiającego i Wykonawców w postępowaniu o udzielenie zamówienia stosuje się przepisy powołanej ustawy PZP oraz aktów wykonawczych wydanych na jej podstawie, a w sprawach nieuregulowanych przepisy ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny (t. j. Dz. U. 2023 poz. 1610 ze zm.).
3. Postępowanie prowadzone jest pod znakiem **80.272.206.2024**, we wszelkiej korespondencji należy powoływać się na przedmiotowy znak sprawy.

Rozdział III - Opis przedmiotu zamówienia.

1. Przedmiotem postępowania i zamówienia jest wyłonienie Wykonawcy w zakresie dostawy 17 000 (siedemnastu tysięcy) licencji na oprogramowanie antywirusowe dla pracowników UJ. Licencja musi być ważna w okresie 1 (jednego) roku od momentu wdrożenia przedmiotu umowy.
2. Szczegółowy opis przedmiotu zamówienia wraz z opisem minimalnych parametrów i wymagań technicznych oraz funkcjonalnych zawiera Załącznik A do SWZ.
3. W przypadku, gdy Wykonawca zapowiada zatrudnienie podwykonawców do oferty musi być załączony wykaz z zakresem powierzonych im zadań (części zamówienia), przy czym niedopuszczalnym jest podzlecanie prac przez podwykonawców dla kolejnych podwykonawców.
4. Opis przedmiotu zamówienia zgodny z nomenklaturą Wspólnego Słownika Zamówień CPV: *48760000-3 – pakiety oprogramowania do ochrony antywirusowej.*

Rozdział IV – Przedmiotowe środki dowodowe

Zamawiający nie wymaga złożenia przedmiotowych środków dowodowych.

Rozdział V - Termin wykonania zamówienia

1. Termin wdrożenia przedmiotu Umowy: do **5 dni kalendarzowych** licząc od dnia udzielenia zamówienia, tj. zawarcia Umowy.
2. Wykonawca zapewnia gotowość do realizacji zamówienia w dniu zawarcia Umowy.

Rozdział VI - Opis warunków podmiotowych udziału w postępowaniu

1. Zdolność do występowania w obrocie gospodarczym – Zamawiający nie wyznacza warunku w tym zakresie.
2. Uprawnienia do prowadzenia określonej działalności gospodarczej lub zawodowej, o ile wynika to z odrębnych przepisów – Zamawiający nie wyznacza warunku w tym zakresie.
3. Sytuacja ekonomiczna lub finansowa – Zamawiający nie wyznacza warunku w tym zakresie.
4. Zdolność techniczna lub zawodowa – Zamawiający nie wyznacza warunku w tym zakresie.

Rozdział VII - Podstawy wykluczenia wykonawców

1. Zamawiający wykluczy wykonawcę w przypadku zaistnienia okoliczności przewidzianych postanowieniami:
   1.1 art. 108 ust. 1 PZP, z zastrzeżeniem art. 110 ust. 2; tj.:
      1.1.1 będącego osobą fizyczną, którego prawomocnie skazano za przestępstwo:
         a) udziału w zorganizowanej grupie przestępczej albo związku mającym na celu popełnienie przestępstwa lub przestępstwa skarbowego, o którym mowa w art. 258 Kodeksu karnego,
         b) handlu ludźmi, o którym mowa w art. 189a Kodeksu karnego,
         c) o którym mowa w art. 228–230a, art. 250a Kodeksu karnego, w art. 46–48 ustawy z dnia 25 czerwca 2010 r. o sporcie (Dz. U. z 2022 r. poz. 1599 i 2185) lub w art. 54 ust. 1–4 ustawy z dnia 12 maja 2011 r. o refundacji leków, środków spożywczych specjalnego przeznaczenia żywieniowego oraz wyrobów medycznych (Dz. U. z 2023 r. poz. 826),
         d) finansowania przestępstwa o charakterze terrorystycznym, o którym mowa w art. 165a Kodeksu karnego, lub przestępstwo udaremniania lub utrudniania stwierdzenia przestępnego pochodzenia pieniędzy lub ukrywania ich pochodzenia, o którym mowa w art. 299 Kodeksu karnego,
         e) o charakterze terrorystycznym, o którym mowa w art. 115 § 20 Kodeksu karnego, lub mające na celu popełnienie tego przestępstwa,
         f) powierzenia wykonywania pracy małoletniemu cudzoziemcowi, o którym mowa w art. 9 ust. 2 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej (Dz. U. z 2021 r. poz. 1745),
         g) przeciwko obrotowi gospodarczemu, o których mowa w art. 296–307 Kodeksu karnego, przestępstwo oszustwa, o którym mowa w art. 286 Kodeksu karnego, przestępstwo przeciwko wiarygodności dokumentów, o których mowa w art. 270–277d Kodeksu karnego, lub przestępstwo skarbowe,
         h) o którym mowa w art. 9 ust. 1 i 3 lub art. 10 ustawy z dnia 15 czerwca 2012 r. o skutkach powierzania wykonywania pracy cudzoziemcom przebywającym wbrew przepisom na terytorium Rzeczypospolitej Polskiej

      – lub za odpowiedni czyn zabroniony określony w przepisach prawa obcego;
      1.1.2 jeżeli urzędującego członka jego organu zarządzającego lub nadzorczego, wspólnika spółki w spółce jawnej lub partnerskiej albo komplementariusza w spółce komandytowej lub komandytowo-akcyjnej lub prokurenta prawomocnie skazano za przestępstwo, o którym mowa w pkt 1;
      1.1.3 wobec którego wydano prawomocny wyrok sądu lub ostateczną decyzję

administracyjną o zaleganiu z uiszczeniem podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenie społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności;

1.1.4 wobec którego prawomocnie orzeczono zakaz ubiegania się o zamówienia publiczne;

1.1.5 jeżeli zamawiający może stwierdzić, na podstawie wiarygodnych przesłanek, że wykonawca zawarł z innymi wykonawcami porozumienie mające na celu zakłócenie konkurencji, w szczególności jeżeli należąc do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, złożyli odrębne oferty, oferty częściowe lub wnioski o dopuszczenie do udziału w postępowaniu, chyba że wykażą, że przygotowali te oferty lub wnioski niezależnie od siebie;

1.1.6 jeżeli, w przypadkach, o których mowa w art. 85 ust. 1, doszło do zakłócenia konkurencji wynikającego z wcześniejszego zaangażowania tego wykonawcy lub podmiotu, który należy z wykonawcą do tej samej grupy kapitałowej w rozumieniu ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów, chyba że spowodowane tym zakłócenie konkurencji może być wyeliminowane w inny sposób niż przez wykluczenie wykonawcy z udziału w postępowaniu o udzielenie zamówienia. Wykonawca nie podlega wykluczeniu w okolicznościach określonych w art. 108 ust. 1 pkt 1, 2 i 5 lub art. 109 ust. 1 pkt 2–5 i 7–10, jeżeli udowodni zamawiającemu, że spełnił łącznie przesłanki, o których mowa w art. 110 ust. 2 ustawy PZP

1.2 art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t. j. Dz. U. 2024 poz. 507 ze zm.) – zwanej dalej „Ustawą sankcyjną”;

2. Stosownie do treści art. 109 ust. 1 ustawy PZP, Zamawiający wykluczy z postępowania Wykonawcę:

2.1 który naruszył obowiązki dotyczące płatności podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne, z wyjątkiem przypadku, o którym mowa w art. 108 ust. 1 pkt 3, chyba że wykonawca odpowiednio przed upływem terminu do składania wniosków o dopuszczenie do udziału w postępowaniu albo przed upływem terminu składania ofert dokonał płatności należnych podatków, opłat lub składek na ubezpieczenia społeczne lub zdrowotne wraz z odsetkami lub grzywnami lub zawarł wiążące porozumienie w sprawie spłaty tych należności (art. 109 ust. 1 pkt 1);

2.2 w stosunku, do którego otwarto likwidację, ogłoszono upadłość, którego aktywami zarządza likwidator lub sąd, zawarł układ z wierzycielami, którego działalność gospodarcza jest zawieszona albo znajduje się on w innej tego rodzaju sytuacji wynikającej z podobnej procedury przewidzianej w przepisach miejsca wszczęcia tej procedury (art. 109 ust.1 pkt 4);

2.3 który w sposób zawiniony poważnie naruszył obowiązki zawodowe, co podważa jego uczciwość, w szczególności gdy Wykonawca w wyniku zamierzonego działania lub rażącego niedbalstwa nie wykonał lub nienależycie wykonał zamówienie, co zamawiający jest w stanie wykazać za pomocą stosownych dowodów w (art. 109 ust. 1 pkt 5);

2.4 który, z przyczyn leżących po jego stronie, w znacznym stopniu lub zakresie nie wykonał lub nienależycie wykonał albo długotrwale nienależycie wykonywał istotne zobowiązanie wynikające z wcześniejszej Umowy w sprawie zamówienia publicznego lub Umowy koncesji, co doprowadziło do wypowiedzenia lub odstąpienia od Umowy, odszkodowania, wykonania zastępczego lub realizacji uprawnień z tytułu rękojmi za wady (art. 109 ust. 1 pkt 7);

2.5 który w wyniku zamierzonego działania lub rażącego niedbalstwa wprowadził zamawiającego w błąd przy przedstawianiu informacji, że nie podlega wykluczeniu, spełnia warunki udziału w postępowaniu lub kryteria selekcji, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia, lub który zataił te informacje

lub nie jest w stanie przedstawić wymaganych podmiotowych środków dowodowych (art. 109 ust. 1 pkt 8);

2.6 który bezprawnie wpływał lub próbował wpływać na czynności zamawiającego lub próbował pozyskać lub pozyskał informacje poufne, mogące dać mu przewagę w postępowaniu o udzielenie zamówienia (art. 109 ust. 1 pkt 9);

2.7 który w wyniku lekkomyślności lub niedbalstwa przedstawił informacje wprowadzające w błąd, co mogło mieć istotny wpływ na decyzje podejmowane przez zamawiającego w postępowaniu o udzielenie zamówienia (art. 109 ust. 1 pkt 10).

3. W przypadkach, o których mowa w ust. 2.1-2.4 niniejszego rozdziału, zamawiający może nie wykluczać Wykonawcy, jeżeli wykluczenie byłoby w sposób oczywisty nieproporcjonalne, w szczególności gdy kwota zaległych podatków lub składek na ubezpieczenie społeczne jest niewielka albo sytuacja ekonomiczna lub finansowa Wykonawcy, o którym mowa w ust. 2.2 powyżej, jest wystarczająca do wykonania zamówienia.

Rozdział VIII - Wykaz oświadczeń i dokumentów, jakie mają dostarczyć Wykonawcy w celu potwierdzenia spełnienia warunków udziału w postępowaniu oraz braku podstaw do wykluczenia.

1. Oświadczenia składane obligatoryjnie wraz z ofertą:
   1.1 W celu potwierdzenia braku podstaw do wykluczenia Wykonawcy z postepowania o udzielenie zamówienia publicznego w okolicznościach, o których mowa w Rozdziale VII SWZ, Wykonawca musi dołączyć do oferty oświadczenie Wykonawcy o niepodleganiu wykluczeniu według wzoru stanowiącego załącznik nr 1 do formularza oferty.
   1.2 Wykonawca, który zamierza powierzyć wykonanie części zamówienia podwykonawcom, w celu wykazania braku istnienia wobec nich podstaw wykluczenia, jest zobowiązany do złożenia oświadczenia, o którym mowa w punkcie 1.1 w części dotyczącej podwykonawców.
   1.3 W przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie w celu potwierdzenia braku podstaw do wykluczenia, o których mowa w punkcie 1.1 składa każdy z wykonawców wspólnie ubiegających się o zamówienie.
2. Dokumenty i oświadczenia, które Wykonawca będzie zobowiązany złożyć na wezwanie Zamawiającego - dotyczy wykonawcy, którego oferta została najwyżej oceniona – *Nie dotyczy.*
3. Jeżeli, w toku postępowania, Wykonawca nie złoży oświadczenia, oświadczeń lub dokumentów niezbędnych do przeprowadzenia postępowania, złożone oświadczenia lub dokumenty są niekompletne, zawierają błędy lub budzą wskazane przez Zamawiającego wątpliwości, Zamawiający wezwie do ich złożenia, uzupełnienia, poprawienia w terminie przez siebie wskazanym, chyba że mimo ich złożenia oferta wykonawcy podlegałaby odrzuceniu albo konieczne byłoby unieważnienie postępowania.

Rozdział IX - Informacja o sposobie porozumiewania się Zamawiającego z Wykonawcami oraz przekazywania oświadczeń i dokumentów, a także wskazanie osób uprawnionych do porozumiewania się z Wykonawcami

1. Informacje ogólne.
   1.1 Postępowanie o udzielenie zamówienia publicznego prowadzone jest przy użyciu narzędzia komercyjnego https://platformazakupowa.pl – adres profilu nabywcy: https://platformazakupowa.pl/pn/uj_edu.
   1.2 Wykonawca przystępując do niniejszego postępowania o udzielenie zamówienia publicznego:
      1.2.1 akceptuje warunki korzystania z https://platformazakupowa.pl określone w regulaminie zamieszczonym w zakładce „Regulamin" oraz uznaje go za wiążący;
      1.2.2 zapozna się z instrukcją korzystania z https://platformazakupowa.pl, a w szczególności z zasadami logowania, składania wniosków o wyjaśnienie treści SWZ, składania ofert oraz dokonywania innych czynności w niniejszym postępowaniu przy użyciu https://platformazakupowa.pl dostępną na https://platformazakupowa.pl – link poniżej: https://drive.google.com/file/d/1Kd1DttbBeiNWt4q4slS4t76lZVKPbkyD/view lub w zakładce: https://platformazakupowa.pl/strona/45-instrukcje oraz będzie ją

stosować.

1.3 Wymagania techniczne i organizacyjne składania ofert, wysyłania i odbierania dokumentów elektronicznych, cyfrowego odwzorowania z dokumentem w postaci papierowej, oświadczeń oraz informacji przekazywanych z ich użyciem opisane zostały na https://platformazakupowa.pl, w regulaminie zamieszczonym w zakładce „Regulamin" oraz instrukcji składania ofert (linki w ust. 1.2.2 powyżej).

1.4 Wielkość plików:

1.4.1 w odniesieniu do oferty – maksymalna liczba plików to 10 po 150 MB każdy;

1.4.2 w przypadku komunikacji – wiadomość do Zamawiającego max. 500 MB;

1.5 Komunikacja między Zamawiającym i Wykonawcami odbywa się **wyłącznie** przy użyciu narzędzia komercyjnego https://platformazakupowa.pl – adres profilu nabywcy: https://platformazakupowa.pl/pn/uj_edu

1.5.1 W celu skrócenia czasu udzielenia odpowiedzi na pytania komunikacja między Zamawiającym a Wykonawcami w zakresie:

a. przesyłania Zamawiającemu pytań do treści SWZ;
b. przesyłania odpowiedzi na wezwanie Zmawiającego do złożenia/poprawienia/uzupełnienia oświadczenia, o którym mowa w art. 125 ust. 1, podmiotowych środków dowodowych, innych dokumentów lub oświadczeń składanych w postępowaniu;
c. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści oświadczenia, o którym mowa w art. 125 ust. 1 lub złożonych podmiotowych środków dowodowych lub innych dokumentów lub oświadczeń składanych w postępowaniu;
d. przesyłania odpowiedzi na wezwanie Zamawiającego do złożenia wyjaśnień dotyczących treści przedmiotowych środków dowodowych;
e. przesłania odpowiedzi na inne wezwania Zamawiającego wynikające z ustawy – Prawo zamówień publicznych;
f. przesyłania wniosków, informacji, oświadczeń Wykonawcy;
g. przesyłania odwołania/innych

odbywa się za pośrednictwem https://platformazakupowa.pl i formularza: „Wyślij wiadomość do Zamawiającego".

Za datę przekazania (wpływu) oświadczeń, wniosków, zawiadomień oraz informacji przyjmuje się datę ich przesłania za pośrednictwem https://platformazakupowa.pl poprzez kliknięcie przycisku: „Wyślij wiadomość do Zamawiającego", po którym pojawi się komunikat, że wiadomość została wysłana do Zamawiającego.

1.5.2 Zamawiający przekazuje Wykonawcom informacje za pośrednictwem https://platformazakupowa.pl. Informacje dotyczące odpowiedzi na pytania, zmiany specyfikacji, zmiany terminu składania i otwarcia ofert Zamawiający zamieszcza na platformie w sekcji: „Komunikaty". Korespondencja, której zgodnie z obowiązującymi przepisami adresatem jest konkretny Wykonawca, będzie przekazywana za pośrednictwem https://platformazakupowa.pl do konkretnego Wykonawcy.

1.5.3 Wykonawca jako podmiot profesjonalny ma obowiązek sprawdzania komunikatów i wiadomości bezpośrednio na https://platformazakupowa.pl przesyłanych przez Zamawiającego, gdyż system powiadomień może ulec awarii lub powiadomienie może trafić do folderu SPAM.

1.5.4 Zamawiający, zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (Dz. U. z 2020 r., poz. 2452), określa niezbędne wymagania sprzętowo-aplikacyjne umożliwiające pracę na https://platformazakupowa.pl, tj.:

a. stały dostęp do sieci Internet o gwarantowanej przepustowości nie mniejszej niż 512 kb/s;

b. komputer klasy PC lub MAC o następującej konfiguracji: pamięć min. 2 GB Ram, procesor Intel IV 2 GHZ lub jego nowsza wersja, jeden z systemów operacyjnych – MS Windows 7, Mac Os x 10 4, Linux, lub ich nowsze wersje;
c. zainstalowana dowolna, inna przeglądarka internetowa niż Internet Explorer;
d. włączona obsługa JavaScript;
e. zainstalowany program Adobe Acrobat Reader lub inny obsługujący format plików .pdf.

1.5.5 Szyfrowanie na https://platformazakupowa.pl odbywa się za pomocą protokołu TLS 1.3.

1.5.6 Oznaczenie czasu odbioru danych przez platformę zakupową stanowi datę oraz dokładny czas (hh:mm:ss) generowany według czasu lokalnego serwera synchronizowanego z zegarem Głównego Urzędu Miar.

1.6 Sposób sporządzenia i przekazania dokumentów elektronicznych oraz cyfrowego odwzorowania z dokumentem w postaci papierowej musi być zgody z wymaganiami określonymi w rozporządzeniu Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie sposobu sporządzania i przekazywania informacji oraz wymagań technicznych dla dokumentów elektronicznych oraz środków komunikacji elektronicznej w postępowaniu o udzielenie zamówienia publicznego lub konkursie (t.j.: Dz. U. 2020 r., poz. 2452 z późn. zm) oraz rozporządzeniu Ministra Rozwoju, Pracy i Technologii z dnia 23 grudnia 2020 r. w sprawie podmiotowych środków dowodowych oraz innych dokumentów lub oświadczeń, jakich może żądać Zamawiający od Wykonawcy (t. j.: Dz. U. 2020 r., poz. 2415 z późn. zm.), tj.:

a. dokumenty lub oświadczenia, w tym oferta, składane są w oryginale w formie elektronicznej przy użyciu kwalifikowanego podpisu elektronicznego lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym. W przypadku składania podpisu kwalifikowanego i wykorzystania formatu podpisu XAdES zewnętrzny, zamawiający wymaga dołączenia odpowiedniej ilości plików, tj. podpisywanych plików z danymi oraz plików podpisu w formacie XAdES. ***Oferta złożona bez opatrzenia właściwym podpisem elektronicznym podlega odrzuceniu na podstawie art. 226 ust. 1 pkt 3 ustawy PZP, z uwagi na niezgodność z art. 63 tej ustawy***;
b. dokumenty wystawione w formie elektronicznej przekazuje się jako dokumenty elektroniczne, zapewniając Zamawiającemu możliwość weryfikacji podpisów;
c. jeżeli oryginał dokumentu, oświadczenia lub inne dokumenty składane w postępowaniu o udzielenie zamówienia, nie zostały sporządzone w postaci dokumentu elektronicznego, wykonawca może sporządzić i przekazać cyfrowe odwzorowanie z dokumentem lub oświadczeniem w postaci papierowej, opatrując je kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, co jest równoznaczne z poświadczeniem przekazywanych dokumentów lub oświadczeń za zgodność z oryginałem;
d. w przypadku przekazywania przez wykonawcę cyfrowego odwzorowania z dokumentem w postaci papierowej, opatrzenie go kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym przez wykonawcę albo odpowiednio przez podmiot, na którego zdolnościach lub sytuacji polega wykonawca na zasadach określonych w art. 118 ustawy PZP, albo przez podwykonawcę jest równoznaczne z poświadczeniem za zgodność z oryginałem.
e. Poświadczenia za zgodność z oryginałem dokonuje odpowiednio wykonawca, podmiot, na którego zdolnościach lub sytuacji polega wykonawca, wykonawcy wspólnie ubiegający się o udzielenie zamówienia publicznego albo podwykonawca, w zakresie dokumentów, które każdego z nich dotyczą (w odniesieniu do pełnomocnictw – zgodnie z zasadą opisaną w rozdziale XII ust. 7 niniejszej SWZ).

2. Sposób porozumiewania się Zamawiającego z Wykonawcami w zakresie skutecznego złożenia oferty.

2.1 Oferta musi być sporządzona z zachowaniem postaci elektronicznej w formacie danych zgodnym z Obwieszczeniem Prezesa Rady Ministrów z dnia 9 listopada 2017 r. w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych i podpisana kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Zaleca się wykorzystanie formatów: ***.pdf, .doc., .xls, .jpg (.jpeg) ze szczególnym wskazaniem na .pdf.*** W celu ewentualnej kompresji danych rekomenduje się wykorzystanie formatów: ***.zip, 7Z***. Do formatów powszechnych a nieobjętych treścią rozporządzenia zalicza się: .rar, .gif, .bmp, .numbers, .pages. Dokumenty złożone w takich plikach zostaną uznane za złożone nieskutecznie.

2.2 Wykonawca składa ofertę za pośrednictwem https://platformazakupowa.pl – adres profilu nabywcy https://platformazakupowa.pl/pn/uj_edu, zgodnie z regulaminem, o którym mowa w ust. 1 tego rozdziału. Zamawiający nie ponosi odpowiedzialności za złożenie oferty w sposób niezgodny z instrukcją korzystania z https://platformazakupowa.pl, w szczególności za sytuację, gdy Zamawiający zapozna się z treścią oferty przed upływem terminu składania ofert (np. złożenie oferty w zakładce „Wyślij wiadomość do zamawiającego"). Taka oferta zostanie uznana przez Zamawiającego za ofertę handlową i nie będzie brana pod uwagę w przedmiotowym postępowaniu, ponieważ nie został spełniony obowiązek narzucony w art. 221 ustawy – Prawo zamówień publicznych.

2.3 Sposób zaszyfrowania oferty opisany został w instrukcji składania ofert (linki w ust. 1.2.2 powyżej), przy czym szyfrowanie ofert ma być dokonywane jedynie za pomocą narzędzia wbudowanego w platformę zakupowa.

2.4 Po upływie terminu składania ofert Wykonawca nie może skutecznie dokonać zmiany ani wycofać uprzednio złożonej oferty.

3. Do porozumiewania z Wykonawcami upoważniony w zakresie formalno-prawnym jest – mgr Piotr Porębski, *tel.: +48 12 663-39-07.*

Rozdział X - Wymagania dotyczące wadium.

1. Zamawiający nie wymaga złożenia wadium.

Rozdział XI - Termin związania ofertą.

1. Wykonawca jest związany złożoną ofertą od dnia upływu terminu składania ofert do dnia **20.08.2024** r. włącznie.
2. W przypadku gdy wybór najkorzystniejszej oferty nie nastąpi przed upływem terminu związania oferta określonego w SWZ, Zamawiający przed upływem terminu związania oferta zwraca się jednokrotnie do Wykonawców o wyrażenie zgody na przedłużenie tego terminu o wskazywany przez niego okres, nie dłuższy niż 30 dni.
3. Przedłużenie terminu związania oferta, o którym mowa w ust. 2, wymaga złożenia przez Wykonawcę pisemnego oświadczenia o wyrażeniu zgody na przedłużenie terminu związania ofertą.

Rozdział XII - Opis sposobu przygotowywania ofert.

1. Każdy wykonawca może złożyć tylko jedną ofertę na realizację całości przedmiotu zamówienia, w formie w elektronicznej, tj. opatrzoną elektronicznym podpisem kwalifikowanym lub w postaci elektronicznej opatrzonej podpisem zaufanym lub podpisem osobistym.
2. Ofertę składa się z zachowaniem formy i sposobu opisanych w Rozdziale IX niniejszej SWZ.
3. Dopuszcza się możliwość złożenia oferty przez dwa lub więcej podmiotów wspólnie ubiegających się o udzielenie zamówienia publicznego na zasadach opisanych w treści art. 58 ustawy PZP.
4. Oferta musi być napisana w języku polskim.
5. Oferta wraz ze wszystkimi jej załącznikami musi być podpisana przez osobę (osoby) uprawnioną do reprezentacji Wykonawcy, zgodnie z wpisem do Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub do innego, właściwego rejestru. Powyższe

dokumenty (wpis do Krajowego Rejestru Sądowego, Centralnej Ewidencji i Informacji o Działalności Gospodarczej lub do innego, właściwego rejestru Wykonawca załącza wraz z ofertą, chyba że zmawiający może uzyskać je za pomocą bezpłatnych i ogólnodostępnych baz danych, a Wykonawca wskazał dane umożliwiające dostęp do tych dokumentów w treści oferty. Jeżeli w imieniu Wykonawcy działa osoba, której umocowanie nie wynika z ww. dokumentów, Wykonawca wraz z ofertą przedkłada pełnomocnictwo lub inny dokument potwierdzający umocowanie do reprezentowania Wykonawcy. Pełnomocnictwa sporządzone w języku obcym Wykonawca składa wraz z tłumaczeniem na język polski.

6. W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia lub w sytuacji reprezentowania Wykonawcy przez pełnomocnika do oferty musi być dołączone pełnomocnictwo. Wraz z pełnomocnictwem winien być złożony dokument potwierdzający możliwość udzielania pełnomocnictwa.
7. Pełnomocnictwo przekazuje się w postaci elektronicznej, opatrzonej kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym. Pełnomocnictwo sporządzone jako dokument w postaci papierowej i opatrzony własnoręcznym podpisem przekazuje się jako cyfrowe odwzorowanie tego dokumentu opatrzone kwalifikowanym podpisem elektronicznym, podpisem zaufanym lub podpisem osobistym, poświadczającym zgodność cyfrowego odwzorowania z dokumentem w postaci papierowej, przy czym poświadczenia dokonuje mocodawca lub notariusz, zgodnie z art. 97 § 2 ustawy z dnia 14 lutego 1991 r. – Prawo o notariacie (t. j. Dz. U. 2022 poz. 1799 ze zm.).
8. Oferta wraz ze stanowiącymi jej integralną część załącznikami musi być sporządzona przez wykonawcę, wedle treści postanowień niniejszej SWZ i jej załączników, a w szczególności musi zawierać:
   8.1 formularz oferty wraz z załącznikami (wypełnionymi i uzupełnionymi lub sporządzonymi zgodnie z ich treścią), w tym:
      8.1.1 oświadczenie Wykonawcy o niepodleganiu wykluczeniu z postępowania – w przypadku wspólnego ubiegania się o zamówienie przez Wykonawców, oświadczenie o niepodleganiu wykluczeniu składa każdy z Wykonawców – załącznik nr 1 do formularza oferty;
      8.1.2 pełnomocnictwo (zgodnie z ust. 5-7 powyżej) lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy;
      8.1.3 wykaz podwykonawców (o ile dotyczy);
      8.1.4 KRS lub CEiDG – o ile nie podano danych do ogólnodostępnych baz.
9. Jeżeli Wykonawca składając ofertę, zastrzega sobie prawo do nie udostępnienia innym uczestnikom postępowania informacji stanowiących tajemnicę przedsiębiorstwa, w rozumieniu przepisów o zwalczaniu nieuczciwej konkurencji, musi to wyraźnie wskazać w ofercie, poprzez złożenie stosownego oświadczenia zawierającego wykaz zastrzeżonych dokumentów i wykazanie, iż zastrzeżone informacje stanowią tajemnice przedsiębiorstwa. Dokumenty opatrzone klauzulą; „Dokument zastrzeżony" winny być załączone łącznie z oświadczeniem i stanowić odrębne pliki zaszyfrowane wraz innymi plikami stanowiącymi ofertę. Wykonawca nie może zastrzec informacji, o których mowa w art. 222 ust. 5 ustawy PZP.
10. Wszystkie koszty związane z przygotowaniem i złożeniem oferty ponosi wykonawca.

Rozdział XIII – Sposób oraz termin składania i otwarcia ofert.

1. Oferty należy składać w terminie **do dnia 22.07.2024 r. do godziny 10:00,** na zasadach, opisanych w rozdziale IX ust. 1-2 SWZ.
2. Wykonawca przed upływem terminu do składania ofert może wycofać ofertę zgodnie z regulaminem na https://platformazakupowa.pl. Sposób wycofania oferty zamieszczono w instrukcji dostępnej pod adresem: https://platformazakupowa.pl/strona/45-instrukcje. Oferta nie może zostać wycofana po upływie terminu składania ofert.
3. Zamawiający odrzuci ofertę złożoną po terminie składania ofert.
4. Otwarcie ofert nastąpi **w dniu 22.07.2024 r. o godzinie 11:00** za pośrednictwem https://platformazakupowa.pl.

5. W przypadku zmiany terminu składania ofert, Zamawiający zamieści informację o jego przedłużeniu na https://platformazakupowa.pl – adres profilu nabywcy – https://platformazakupowa.pl/pn/uj_edu, w zakładce właściwej dla prowadzonego postępowania, w sekcji „Komunikaty".
6. W przypadku awarii systemu teleinformatycznego, skutkującej brakiem możliwości otwarcia ofert w terminie określonym przez Zamawiającego, otwarcie ofert nastąpi niezwłocznie po usunięciu awarii.
7. Zamawiający najpóźniej przed otwarciem ofert udostępni na https://platformazakupowa.pl – adres profilu nabywcy – https://platformazakupowa.pl/pn/uj_edu, w zakładce właściwej dla prowadzonego postępowania, w sekcji „Komunikaty", informację o kwocie, jaką zamierza przeznaczyć na sfinansowanie zamówienia.
8. Zamawiający niezwłocznie po otwarciu ofert, udostępni na stronie internetowej prowadzonego postępowania informacje o:
   8.1 nazwach albo imionach i nazwiskach oraz siedzibach lub miejscach prowadzonej działalności gospodarczej, albo miejscach zamieszkania wykonawców, których oferty zostały otwarte;
   8.2 cenach lub kosztach zawartych w ofertach.
9. Zamawiający nie przewiduje przeprowadzania jawnej sesji otwarcia ofert z udziałem wykonawców, jak też transmitowania sesji otwarcia za pośrednictwem elektronicznych narzędzi do przekazu wideo on-line.

Rozdział XIV - Opis sposobu obliczenia ceny.

1. Cenę oferty należy podać w złotych polskich, uwzględniając podatki oraz rabaty, upusty itp., których wykonawca zamierza udzielić oraz wszystkie koszty związane z realizacją Umowy.
2. Nie przewiduje się żadnych przedpłat ani zaliczek na poczet realizacji przedmiotu Umowy.
3. Ceny muszą być podane i wyliczone w zaokrągleniu do dwóch miejsc po przecinku (zasada zaokrąglenia – poniżej 5 należy końcówkę pominąć, powyżej i równe 5 należy zaokrąglić w górę).
4. Zamawiający przewiduje płatność zgodnie z postanowieniami załączonego do niniejszej SWZ wzoru Umowy.
5. Jeżeli złożono ofertę, której wybór prowadziłby do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług, zamawiający w celu oceny takiej oferty dolicza do przedstawionej w niej ceny podatek od towarów i usług, który miałby obowiązek rozliczyć zgodnie z tymi przepisami.
6. W przypadku złożenia oferty przez Wykonawcę niezobowiązanego bądź zwolnionego z obowiązku odprowadzania podatku od towarów i usług VAT, podczas czynności porównania ofert, zamawiający doliczy do zaoferowanej przez ww. Wykonawcę ceny stosowny podatek, do uiszczenia którego będzie obowiązany. W tym wypadku koszt podatku pokrywa Zamawiający.
7. Wykonawca, składając ofertę, informuje zamawiającego, czy wybór oferty będzie prowadzić do powstania u zamawiającego obowiązku podatkowego, wskazując nazwę (rodzaj) towaru lub usługi, których dostawa lub świadczenie będzie prowadzić do jego powstania, oraz wskazując ich wartość bez kwoty podatku.

Rozdział XV - Opis kryteriów, którymi Zamawiający będzie się kierował przy wyborze oferty wraz z podaniem znaczenia tych kryteriów i sposobu oceny ofert.

1. Kryterium oceny ofert:
   1.1 Cena brutto za całość przedmiotu zamówienia– 100%
2. Punkty przyznawane za kryterium „Cena brutto za całość przedmiotu zamówienia", będą liczone wg następującego wzoru:

   C = (Cnaj /Co) x 100
   gdzie:
   C – liczba punktów przyznana danej ofercie.
   Cnaj – najniższa cena spośród ważnych ofert.
   Co – cena podana przez Wykonawcę, dla którego wynik jest obliczany.

Maksymalna liczba punktów do uzyskania w tym kryterium przez Wykonawcę wynosi 100.

3. Wszystkie obliczenia punktów będą dokonywane z dokładnością do dwóch miejsc po przecinku (bez zaokrągleń).
4. Oferta Wykonawcy, która uzyska najwyższą liczbę punktów, uznana zostanie za najkorzystniejszą.
5. Jeżeli zostały złożone oferty o takiej samej cenie, Zamawiający wzywa Wykonawców, którzy złożyli te oferty, do złożenia w terminie określonym przez zamawiającego ofert dodatkowych.

Rozdział XVI - Informację o formalnościach, jakie powinny zostać dopełnione po wyborze oferty w celu zawarcia Umowy w sprawie zamówienia publicznego.

1. Przed podpisaniem Umowy Wykonawca powinien złożyć:
   1.1 kopię Umowy(-ów) określającej podstawy i zasady wspólnego ubiegania się o udzielenie zamówienia publicznego – w przypadku złożenia oferty przez podmioty występujące wspólnie (tj. konsorcjum);
   1.2 wykaz podwykonawców z zakresem powierzanych im zadań, o ile przewiduje się ich udział w realizacji zamówienia;
   1.3 oświadczenie o niepodleganiu wykluczeniu – art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t. j. Dz. U. 2024 poz. 507 ze zm.) – w przypadku wykonawców wspólnie ubiegających się o zamówienie oświadczenie składa każdy z nich;
2. Wybrany Wykonawca jest zobowiązany do zawarcia Umowy w terminie i miejscu wyznaczonym przez Zamawiającego.

Rozdział XVII - Wymagania dotyczące zabezpieczenia należytego wykonania Umowy.

Zamawiający nie przewiduje konieczności wniesienia zabezpieczenia należytego wykonania Umowy.

Rozdział XVIII - Wzór Umowy – Załącznik nr 2 do SWZ.

Rozdział XIX - Pouczenie o środkach ochrony prawnej przysługujących Wykonawcy w toku postępowania o udzielenie zamówienia.

1. Środki ochrony prawnej przysługują Wykonawcy, jeżeli ma lub miał interes w uzyskaniu zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez Zamawiającego przepisów ustawy PZP.
2. Odwołanie przysługuje na:
   1.1 niezgodna z przepisami ustawy czynność Zamawiającego, podjętą w postepowaniu o udzielenie zamówienia, w tym na projektowane postanowienie Umowy;
   1.2 zaniechanie czynności w postepowaniu o udzielenie zamówienia, do której Zamawiający był obowiązany na podstawie ustawy PZP.
3. Odwołanie wnosi się do Prezesa Krajowej Izby Odwoławczej w formie pisemnej albo w formie elektronicznej, albo w postaci elektronicznej opatrzone podpisem zaufanym.
4. Na orzeczenie Krajowej Izby Odwoławczej oraz postanowienie Prezesa Krajowej Izby Odwoławczej, o którym mowa w art. 519 ust. 1 ustawy PZP, stronom oraz uczestnikom postepowania odwoławczego przysługuje skarga do sadu. Skargę wnosi się do Sądu Okręgowego w Warszawie, – sądu zamówień publicznych, za pośrednictwem Prezesa Krajowej Izby Odwoławczej.
5. Szczegółowe informacje dotyczące środków ochrony prawnej określone są w Dziale IX „Środki ochrony prawnej" ustawy PZP.

Rozdział XX - Postanowienia ogólne.

1. Zamawiający nie dopuszcza składania ofert częściowych.
2. Powody niedokonania podziału zamówienia na części: zamówienie jest niepodzielne.
3. Zamawiający nie przewiduje możliwości zawarcia Umowy ramowej.

4. Zamawiający nie przewiduje możliwości udzielenie zamówienia polegającego na powtórzeniu podobnych dostaw podstawie art. 214 ust. 1 pkt 8 ustawy PZP.
5. Zamawiający nie dopuszcza składania ofert wariantowych.
6. Rozliczenia pomiędzy Wykonawcą a Zamawiającym będą dokonywane w złotych polskich (PLN).
7. Zamawiający nie przewiduje aukcji elektronicznej.
8. Zamawiający nie przewiduje zwrotu kosztów udziału w postępowaniu.
9. Zamawiający żąda wskazania w ofercie przez wykonawcę tego zakresu zamówienia, odpowiednio do treści postanowień SWZ, którego wykonanie zamierza powierzyć podwykonawcom.

Rozdział XXI - Informacja o przetwarzaniu danych osobowych - dotyczy Wykonawcy będącego osobą fizyczną.

Zgodnie z art. 13 i 14 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, dalej „RODO") w zw. z art. 19 ust. 1 ustawy PZP, Uniwersytet Jagielloński informuje, że:

1. **Administratorem** Pani/Pana danych osobowych jest Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków, reprezentowany przez Rektora UJ.
2. **Uniwersytet Jagielloński wyznaczył Inspektora Ochrony Danych**, ul. Czapskich 4, 31-110 Kraków, pokój nr 27. Kontakt z Inspektorem możliwy jest przez e-mail: iod@uj.edu.pl lub pod nr telefonu +4812 663 12 25.
3. Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c) RODO w celu związanym z postępowaniem o udzielenie zamówienia publicznego, *nr sprawy 80.272.206.2024*
4. Podanie przez Panią/Pana danych osobowych jest wymogiem ustawowym określonym w przepisach ustawy PZP związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego.
5. Konsekwencje niepodania danych osobowych wynikają z ustawy PZP.
6. Odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym udostępniona zostanie dokumentacja postępowania w oparciu o art. 18 oraz art. 74 ust. 3 oraz 4 ustawy PZP, przy czym udostępnieniu nie podlegają dane osobowe, o których mowa w art. 9 ust. 1 RODO, zebrane w toku postępowania o udzielenie zamówienia.
7. Pani/Pana dane osobowe będą przechowywane zgodnie z art. 78 ust. 1 ustawy PZP przez okres co najmniej 4 lat liczonych od dnia zakończenia postępowania o udzielenie zamówienia publicznego albo do upływu terminu możliwości kontroli projektu współfinansowanego lub finansowanego ze środków Unii Europejskiej albo jego trwałości takie projektu bądź innych umów czy zobowiązań wynikających z realizowanych projektów.
8. Posiada Pani/Pan prawo do:
   8.1 na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących;
   8.2 na podstawie art. 16 RODO prawo do sprostowania Pani/Pana danych osobowych;
   8.3 na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych;
   8.4 prawo do wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.
9. Nie przysługuje Pani/Panu prawo do:
   9.1 prawo do usunięcia danych osobowych w zw. z art. 17 ust. 3 lit. b), d) lub e) RODO,
   9.2 prawo do przenoszenia danych osobowych, o którym mowa w art. 20 RODO,
   9.3 prawo sprzeciwu, wobec przetwarzania danych osobowych, gdyż podstawą prawną przetwarzania Pani/Pana danych osobowych jest art. 6 ust. 1 lit. c) w zw. z art. 21 RODO.
10. **Pana/Pani dane osobowe, o których mowa w art. 10 RODO**, mogą zostać udostępnione, w celu umożliwienia korzystania ze środków ochrony prawnej, o których mowa w Dziale IX ustawy PZP, do upływu terminu na ich wniesienie.

11. Zamawiający informuje, że **w odniesieniu do Pani/Pana danych osobowych** decyzje nie będą podejmowane w sposób zautomatyzowany, stosownie do art. 22 RODO.
12. W przypadku gdy wykonanie obowiązków, o których mowa w art. 15 ust. 1– 3 RODO, celem realizacji Pani/Pana uprawnienia wskazanego pkt 8 lit. a) powyżej, wymagałoby niewspółmiernie dużego wysiłku, **zamawiający może żądać od Pana/Pani**, wskazania dodatkowych informacji mających na celu sprecyzowanie żądania, w szczególności podania nazwy lub daty wszczętego albo zakończonego postępowania o udzielenie zamówienia publicznego.
13. **Skorzystanie przez Panią/Pana**, z uprawnienia wskazanego pkt 8 lit. b) powyżej, do sprostowania lub uzupełnienia danych osobowych, o którym mowa w art. 16 RODO, nie może skutkować zmianą wyniku postępowania o udzielenie zamówienia publicznego, ani zmianą postanowień Umowy w zakresie niezgodnym z ustawą PZP, ani nie może naruszać integralności protokołu postępowania udzielenie zamówienia publicznego oraz jego załączników.
14. **Skorzystanie przez Panią/Pana**, z uprawnienia wskazanego pkt 8 lit. c) powyżej, polegającym na żądaniu ograniczenia przetwarzania danych, o którym mowa w art. 18 ust. 1 RODO, nie ogranicza przetwarzania danych osobowych do czasu zakończenia postępowania o udzielenie zamówienia publicznego oraz również po postępowania w przypadku wystąpienia okoliczności, o których mowa w art. 18 ust. 2 RODO (*prawo do ograniczenia przetwarzania nie ma zastosowania w odniesieniu do przechowywania, w celu zapewnienia korzystania ze środków ochrony prawnej lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego*).

Rozdział XXII - Załączniki do SWZ

Załącznik nr 1 – Formularz oferty;
Załącznik nr 2 – Projektowane postanowienia Umowy
Załącznik A – Szczegółowy Opis Przedmiotu Zamówienia.

Nr sprawy: 80.272.206.2024

Załącznik nr 1 do SWZ

FORMULARZ OFERTY - Znak sprawy 80.272.206.2024

ZAMAWIAJĄCY: ***Uniwersytet Jagielloński***
ul. Gołębia 24, 31 – 007 Kraków
Jednostka prowadząca sprawę: ***Dział Zamówień Publicznych UJ***
ul. Straszewskiego 25/3 i 4, 31-113 Kraków

Nazwa (Firma) wykonawcy:

.....
.....

Adres siedziby:

.....
.....

Adres do korespondencji:

.....
.....

Kontakt:

tel.: .....
fax: .....
e-mail: .....

Inne dane:

*NIP / PESEL *:* .....
REGON: .....

Dane umożliwiające dostęp do dokumentów potwierdzających umocowanie osoby działającej w imieniu wykonawcy (należy zaznaczyć właściwe i ewentualnie uzupełnić):

☐ *wyszukiwarka KRS:* https://ekrs.ms.gov.pl/web/wyszukiwarka-krs/strona-glowna/,

☐ *przeglądanie wpisów CEIDG:* https://aplikacja.ceidg.gov.pl/ceidg/ceidg.public.ui/search.aspx,

☐ *znajdują się w bezpłatnych i ogólnodostępnych bazach danych dostępnych pod następującym adresem internetowym (podać adres internetowy):* https://.....,

☐ *znajdują się w dokumencie/tach dołączonym/ch do oferty.*

Nawiązując do ogłoszonego postępowania prowadzonego w trybie podstawowym na Wyłonienie Wykonawcy w zakresie dostawy 17 000 (siedemnastu tysięcy) licencji na oprogramowanie antywirusowe dla pracowników UJ, 80.272.206.2024, składamy poniższą ofertę:

1) oferujemy wykonanie **CAŁOŚCI PRZEDMIOTU ZAMÓWIENIA** za maksymalną kwotę netto ……*, plus należny podatek VAT w wysokości …..... * %, co daje kwotę brutto …..... * (słownie: ……..... *).
2) oświadczamy, że oferujemy przedmiot zamówienia zgodny z wymaganiami i warunkami określonymi przez Zamawiającego w SWZ i potwierdzamy przyjęcie warunków umownych i warunków płatności zawartych w SWZ i w projektowanych postanowieniach umownych stanowiącym załącznik do SWZ,
3) oświadczamy, iż oferujemy wykonanie przedmiotu zamówienia w terminie wskazanym w Rozdziale V SWZ,
4) oświadczamy, że wybór oferty:
   - nie będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług. *

- będzie prowadził do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług. Powyższy obowiązek podatkowy będzie dotyczył (tak zwany „odwrócony VAT") ……..…… (*Wpisać nazwę /rodzaj towaru lub usługi, które będą prowadziły do powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług)* objętych przedmiotem zamówienia. *

5) oferujemy termin płatności wynoszący do 30 dni liczony od doręczenia faktury odpowiednio dla wymagań określonych w SWZ,
6) w przypadku przyznania zamówienia – zobowiązujemy się do zawarcia Umowy w miejscu i terminie wyznaczonym przez Zamawiającego,
7) oświadczamy, że uważamy się za związanych niniejszą ofertą na czas wskazany w Rozdz. XI SWZ,
8) oświadczamy, że wypełniliśmy obowiązki informacyjne przewidziane w art. 13 lub art. 14 *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* wobec osób fizycznych, od których dane osobowe bezpośrednio lub pośrednio pozyskaliśmy w celu ubiegania się o udzielenie zamówienia publicznego w niniejszym postępowaniu,
9) oświadczam, że jestem (należy wybrać z listy):
   ☐ mikroprzedsiębiorstwem,
   ☐ małym przedsiębiorstwem,
   ☐ średnim przedsiębiorstwem,
   ☐ jednoosobową działalność gospodarcza,
   ☐ osobą fizyczną nieprowadząca działalności gospodarczej,
   ☐ inny rodzaj ……
10) w przypadku udzielenia zamówienia – zobowiązujemy się do zawarcia Umowy w miejscu i terminie wyznaczonym przez Zamawiającego,
11) osobą upoważnioną do kontaktów z zamawiającym w zakresie złożonej oferty oraz w sprawach związanych z realizacją zamówienia jest:
    .....……
    *[*wypełnić dane personalne i adresowe – tel.; e-mail]*
12) załącznikami do niniejszego formularza oferty są:
    - *Załącznik nr 1* – oświadczenie Wykonawcy o niepodleganiu wykluczeniu,
    - *Załącznik nr 2* – wykaz podwykonawców (o ile dotyczy),
    - *Inne:*
        a. pełnomocnictwo (zgodnie z ust. 5-7 rozdziału XII) lub inny dokument potwierdzający umocowanie do reprezentowania wykonawcy;
        b. KRS lub CEiDG – o ile nie podano danych do ogólnodostępnych baz;

Uwaga! Miejsca wykropkowane i/lub oznaczone „*" we wzorze formularza oferty i wzorach jego załączników Wykonawca zobowiązany jest odpowiednio do ich treści wypełnić lub skreślić.

Załącznik nr 1 do formularza oferty

OŚWIADCZENIE
O NIEPODLEGANIU WYKLUCZENIU Z POSTĘPOWANIA

Składając ofertę w postępowaniu na wyłonienie Wykonawcy w zakresie dostawy licencji na oprogramowanie antywirusowe dla pracowników UJ, 80.272.206.2024:

I. OŚWIADCZENIA DOTYCZĄCE WYKONAWCY

1. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 108 ust. 1 ustawy PZP.
2. Oświadczam, że nie podlegam wykluczeniu z postępowania na podstawie art. 109 ust. 1 pkt 1, 4. 5, i od 7 do 10 ustawy PZP.
3. Oświadczam, iż nie podlegam wykluczeniu na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t. j. Dz. U. 2024 poz. 507 ze zm.), tj.:
   1) nie jestem wykonawcą wymienionym w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 ani wpisanym na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 cyt. ustawy;
   2) nie jestem wykonawcą, którego beneficjentem rzeczywistym w rozumieniu ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U z 2023 r., poz. 1124, 1285,1723 i 1843) jest osoba wymieniona w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 ani wpisana na listę lub będąca takim beneficjentem rzeczywistym od dnia 24 lutego 2022 r., o ile została wpisana na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 cyt. ustawy;
   3) nie jestem wykonawcą, którego jednostką dominującą w rozumieniu art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz.U. z 2023 r., poz. 120,295 i 1598), jest podmiot wymieniony w wykazach określonych w rozporządzeniu 765/2006 i rozporządzeniu 269/2014 albo wpisany na listę lub będący taką jednostką dominującą od dnia 24 lutego 2022 r., o ile został wpisany na listę na podstawie decyzji w sprawie wpisu na listę rozstrzygającej o zastosowaniu środka, o którym mowa w art. 1 pkt 3 cyt. ustawy;

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. ……. ustawy PZP *(podać mającą zastosowanie podstawę wykluczenia spośród wskazanych powyżej).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy PZP podjąłem następujące środki naprawcze:

……..……

….....…….

…….....……

Oświadczam, że zachodzą w stosunku do mnie podstawy wykluczenia z postępowania na podstawie art. 7 ust. 1 ustawy z dnia 13 kwietnia 2022 r. o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego (t. j. Dz. U. 2024 poz. 507 ze zm.), *(podać mającą zastosowanie podstawę wykluczenia spośród wskazanych powyżej)*

……..……

….....…….

II. OŚWIADCZENIE DOTYCZĄCE PODWYKONAWCY NIEBĘDĄCEGO

PODMIOTEM, NA KTÓREGO ZASOBY POWOŁUJE SIĘ WYKONAWCA*

Oświadczam, że w stosunku do następującego/ych podmiotu/tów, będącego/ych podwykonawcą/ami: *(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*,
……..…..……
nie zachodzą podstawy wykluczenia z postępowania o udzielenie zamówienia.

OŚWIADCZENIE

Oświadczam, że w stosunku do podmiotu …… *(należy podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)*
zachodzą podstawy wykluczenia z postępowania na podstawie art. ……. ustawy PZP *(podać mającą zastosowanie podstawę wykluczenia spośród wskazanych powyżej).* Jednocześnie oświadczam, że w związku z ww. okolicznością, na podstawie art. 110 ust. 2 ustawy PZP podjęte zostały następujące środki naprawcze:
……..……
….....…….
…….....……
……..…….....……...

Oświadczam, że wszystkie informacje podane w powyższych oświadczeniach są aktualne i zgodne z prawdą oraz zostały przedstawione z pełną świadomością konsekwencji wprowadzenia Zamawiającego w błąd przy przedstawianiu informacji.

Nr sprawy: 80.272.206.2024

Załącznik nr 2 do formularza oferty

(Pieczęć firmowa Wykonawcy)

OŚWIADCZENIE
(wykaz podwykonawców)

Oświadczamy, że:

- powierzamy* następującym podwykonawcom wykonanie następujących części (zakresu) zamówienia

1. Podwykonawca *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* -
……..
zakres zamówienia:
…….....

2. Podwykonawca *(podać pełną nazwę/firmę, adres, a także w zależności od podmiotu: NIP/PESEL, KRS/CEiDG)* -
…….
zakres zamówienia:
…….....

- nie powierzamy* podwykonawcom żadnej części (zakresu) zamówienia

(jeżeli Wykonawca nie wykreśli żadnej z powyższych opcji, Zamawiający uzna, że nie powierza podwykonawcom wykonania żadnych prac objętych niniejszym zamówieniem)

** niepotrzebne skreślić*

Załącznik nr 2 do SWZ

UMOWA 80.272.206.2024
– wzór (projektowane postanowienia Umowy)

zawarta w Krakowie w dniu ..... r. pomiędzy:
Uniwersytetem Jagiellońskim z siedzibą przy ul. Gołębiej 24, 31-007 Kraków, NIP 675-000-22-36, zwanym dalej „Zamawiającym", reprezentowanym przez:
……. – …….. UJ, przy kontrasygnacie finansowej Kwestora UJ
a
……, wpisanym do ……., NIP: ……., REGON: ……, zwanym dalej „Wykonawcą", reprezentowanym przez:
1. ……..

W wyniku przeprowadzenia postępowania w trybie podstawowym bez negocjacji, zgodnie z art. 275 pkt 1 ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t. j. Dz. U. 2023 poz. 1605 ze zm.), zwaną dalej ustawą PZP, zawarto Umowę następującej treści

§ 1

1. Zamawiający powierza a Wykonawca przyjmuje do zrealizowania przedmiot Umowy polegający na dostawie 17 000 (słownie: siedemnastu tysięcy) licencji na oprogramowanie antywirusowe dla pracowników UJ, zwanej dalej Oprogramowaniem, która będzie ważna w okresie 1 (jednego) roku od momentu wdrożenia przedmiotu umowy.
2. Wykonawca oświadcza, że przedmiot Umowy wskazany w ust. 1 powyżej jest wolny od wad prawnych w rozumieniu art. 556^3 KC, uniemożliwiających Zamawiającemu niezakłócone korzystanie.
3. Wykonawca udziela rękojmi za wady prawne przedmiotu Umowy przez cały okres obowiązywania Umowy wskazany w ust. 9 niniejszego paragrafu Umowy.
4. Jeżeli sąd w wydanym prawomocnym wyroku stwierdzi, że Oprogramowanie ma wady prawne, Zamawiający może od Umowy odstąpić i żądać naprawienia poniesionej rzeczywistej szkody.
5. Do zasad odpowiedzialności Wykonawcy za wady prawne Oprogramowania, w zakresie nieuregulowanym postanowieniami niniejszego paragrafu Umowy stosuje się art. 55 ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t. j. Dz. U. 2022 poz. 2509 ze zm.) oraz Działu II Tytułu XI Księgi III ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2023 poz. 1610 ze zm.).
6. Udzielona licencja obejmuje obszar geograficzny krajów Europejskiego Obszaru Geograficznego (EOG) w zakresie przetwarzania i przechowywania (składowania) danych.
7. Wykonawca udziela **12 miesięcznej rękojmi za wady prawne Oprogramowania**, liczone od dnia, w którym Zamawiający dowiedział się o istnieniu wady prawnej, a jeżeli dowiedział się on o istnieniu wady dopiero na skutek powództwa osoby trzeciej – od dnia, w którym orzeczenie wydane w sporze z osobą trzecią stało się prawomocne.
8. Przedmiot Umowy będzie realizowany w terminie **1 (jednego) roku licząc od momentu wdrożenia przedmiotu Umowy w sposób wskazany w ust. 17 poniżej.**
9. Zamawiający zleca a Wykonawca zobowiązuje się wykonać wszelkie niezbędne czynności dla zrealizowania przedmiotu Umowy określonego w ust. 1.
10. Szczegółowy opis przedmiotu zamówienia zawiera SWZ wraz z załącznikami i ofertą Wykonawcy z dnia …… 2024 r.
11. Strony na potrzeby niniejszej Umowy nadają poniższym wyrażeniom, następujące znaczenie:

11.1 Oprogramowanie" – oznacza program komputerowy/programy komputerowe będący/będące przedmiotem Licencji;

11.2 „Producent" - osoba fizyczna lub prawna, której przysługują majątkowe autorskie prawa do Oprogramowania,

11.3 „Protokół Odbioru" - oznacza dokument podpisany przez przedstawicieli obu Stron sporządzony po Dostawie Oprogramowania, stwierdzający prawidłowość wykonania Dostawy Oprogramowania oraz zgodność Oprogramowania ze specyfikacją zawartą w Ofercie.

12. Wykonawca zapewnia, że subskrypcja na licencje dostarczona Zamawiającemu będzie pochodziła bezpośrednio od Producenta lub z oficjalnych i autoryzowanych przez Producenta kanałów dystrybucyjnych.

13. Wykonawca jest zobowiązany do:

13.1 niezwłocznego zgłaszania Zamawiającemu, w formie pisemnej lub za pośrednictwem poczty elektronicznej Zamawiającego dostępnej pod adresem wskazanym w ust. 18.1 niniejszego paragrafu Umowy faktów naruszania postanowień Umowy,

13.2 przesyłania drogą elektroniczną na adres wskazany w ust. 18.1 niniejszego paragrafu Umowy informacje o aktualizacjach Oprogramowania lub o nowych jego wersjach,

13.3 udzielania, na żądanie Zamawiającego, bezpłatnych informacji o funkcjonowaniu, opcjach albo zakresie działania Oprogramowania.

14. Wykonawca zobowiązuje się do przestrzegania, w trakcie realizacji Umowy, przepisów powszechnie obowiązującego prawa, które odnoszą się do przedmiotu Umowy.

15. Zamawiający zobowiązany jest do korzystania z Oprogramowania zgodnie z Umową oraz Warunkami licencji.

16. Zamawiający oświadcza, iż jako uczelnia publiczna jest uprawniony do korzystania z „licencji" na warunkach przewidzianych dla jednostek edukacyjnych i akademickich.

17. Wykonawca **w terminie do 5 dni kalendarzowych od dnia zawarcia Umowy, wdroży Oprogramowanie** poprzez przekazanie Zamawiającemu dokument potwierdzenia udzielenia subskrypcji na licencję na Oprogramowanie w formie elektronicznej oraz papierowej, a także, jeżeli specyfika Licencji tego wymaga, kody niezbędne do zarejestrowania i uruchomienia Oprogramowania na stronie internetowej.

18. Strony ustalają, że przedstawicielami Zamawiającego w toku realizacji Umowy będą:

18.1 ze strony Zamawiającego: ……., nr telefonu: ……., adres e-mail: …….

18.2 ze strony Wykonawcy: ……., nr telefonu: ……., adres e-mail: …….

19. Osoby wymienione w ust. 19 powyżej, nie są upoważnione do podejmowania decyzji powodujących zmianę postanowień Umowy, w szczególności wzrostu uzgodnionego wynagrodzenia i zwiększenia lub zmiany zakresu przedmiotu Umowy, chyba, że przedstawiciel Zamawiającego jest umocowany do reprezentacji Uniwersytetu Jagiellońskiego w Krakowie, zaś przedstawiciel Wykonawcy wchodzi w skład Zarządu, jest wspólnikiem/partnerem/komplementariuszem Spółki albo jest przedsiębiorcą prowadzącym działalność gospodarczą wpisanym do CEIDG.

20. Integralną częścią niniejszej Umowy jest:

20.1 dokumentacja zamówienia, w tym w szczególności SWZ wraz z załącznikami i ofertą Wykonawcy z dnia …… 2024 r.,

20.2 Załącznik nr 1 – Warunki licencji na Oprogramowane określone przez jego Producenta, w zakresie w jakim nie są one sprzeczne z postanowieniami niniejszej Umowy oraz zapisami SWZ wraz z załącznikami,

20.3 Załącznik nr 2 – Protokół Odbioru przedmiotu Umowy.

§ 2

1. Wykonawca oświadcza, że posiada odpowiednią wiedzę, doświadczenie i dysponuje stosowną bazą do wykonania przedmiotu Umowy, jak również dotrzyma umówionych terminów, przy zachowaniu należytej staranności, uwzględniając zawodowy charakter prowadzonej przez niego działalności.

2. Przedmiot Umowy będzie realizowany przez Wykonawcę siłami własnymi / z udziałem podwykonawców.
3. Wykonawca ponosi całkowitą odpowiedzialność materialną i prawną za powstałe u Zamawiającego, jak i osób trzecich, szkody spowodowane działaniem lub zaniechaniem Wykonawcy lub osób, którymi się posługuje przy realizacji niniejszej Umowy.
4. Zlecenie wykonania części Umowy podwykonawcom nie zmienia zobowiązań Wykonawcy wobec Zamawiającego za wykonanie tej części Umowy. Wykonawca jest odpowiedzialny za działania, uchybienia i zaniedbania podwykonawców i ich pracowników w takim samym stopniu, jakby to były działania, uchybienia lub zaniedbania własne.

§ 3

1. Wysokość wynagrodzenia przysługującego Wykonawcy za wykonanie przedmiotu Umowy ustalona została na podstawie oferty Wykonawcy.
2. Wynagrodzenie za przedmiot Umowy ustala się na kwotę netto: …… PLN (słownie: …… $^{00}/_{100}$), a wraz z należnym podatkiem od towarów i usług VAT w wysokości …% na kwotę brutto …… PLN (słownie: ……. $^{00}/_{100}$).
3. Wynagrodzenie określone w ust. 2 obejmuje wszystkie koszty, które Wykonawca powinien był przewidzieć w celu prawidłowego wykonania Umowy.
4. Zamawiający jest podatnikiem VAT i posiada NIP 675-000-22-36.
5. Wykonawca jest podatnikiem VAT i posiada NIP ..... lub nie jest podatnikiem VAT na terytorium Rzeczypospolitej Polskiej.
6. Należny od kwoty wynagrodzenia podatek od towarów i usług VAT, pokryje Zamawiający na konto właściwego Urzędu Skarbowego w przypadku powstania u Zamawiającego obowiązku podatkowego zgodnie z przepisami o podatku od towarów i usług.[1]

§ 4

1. Wynagrodzenie określone w § 3 ust. 2 Umowy Wykonawca otrzyma, po uruchomieniu licencji na Oprogramowania stanowiącego przedmiot Umowy, co potwierdzone w sposób wskazany w § 1 ust. 17 niniejszej Umowy, na podstawie prawidłowo wystawionej Zamawiającemu faktury oraz podpisaniu Protokołu Odbioru niezawierającego zastrzeżeń.
2. Faktura będzie wystawiona w następujący sposób:
   Uniwersytet Jagielloński, ul. Gołębia 24, 31-007 Kraków NIP 675-000-22-36,
   przy czym fakturę należy złożyć w siedzibie Działu Usług Informatycznych UJ w Krakowie (31-007) przy ul. Gołębiej 24.
3. Termin zapłaty faktury za wykonany i odebrany przedmiot Umowy ustala się **do 30 dni** od daty dostarczenia prawidłowo wystawionej faktury do siedziby Zamawiającego wraz z podpisanym bez zastrzeżeń Protokołem Odbioru.
4. Za dzień odbioru przedmiotu Umowy Strony uważać będą dzień faktycznej realizacji przez Wykonawcę wszelkich czynności składających się na cały przedmiot zamówienia, który zostanie odnotowany w protokole, to jest po przekazaniu Zamawiającemu dokumentu potwierdzającego udzielenie subskrypcji na licencję na Oprogramowanie w formie elektronicznej oraz papierowej, a także, jeżeli specyfika Licencji tego wymaga, kody niezbędne do zarejestrowania i uruchomienia Oprogramowania na stronie internetowej.
5. Odbiór subskrypcji na licencje zostanie potwierdzony podpisaniem Protokołu Odbioru przez osoby upoważnione przez Strony po uruchomieniu subskrypcji przez co Strony rozumieją dzień umożliwienia Zamawiającemu dostępu do Oprogramowania za pośrednictwem strony internetowej wskazanej w § 1 ust. 17 oraz ust. 4 niniejszego paragrafu Umowy.
6. Zamawiający przed podpisaniem Protokołu Odbioru dokona oceny poprawności wykonania przedmiotu Umowy. jeśli Zamawiający stwierdzi nieprawidłowości w zakresie funkcjonowania Oprogramowania i/lub jego niezgodności ze SWZ, Załącznikiem A do SWZ lub ofertą Wykonawcy,

[1] *Jeżeli dotyczy.*

wówczas Zamawiający odmówi dokonania odbioru zaznaczając ten fakt na Protokole Odbioru. W takim przypadku Strony odnotują w Protokole Odbioru wykaz niezgodności z przedmiotem Umowy.

7. Wykonawca zobowiązuje się do usunięcia niezgodności określonych w Protokole Odbioru w terminie 14 dni od dnia sporządzenia Protokołu Odbioru. Podpisanie ostatecznego Protokołu Odbioru może nastąpić dopiero po stwierdzeniu przez Zamawiającego usunięcia wad.
8. Podpisanie protokołu nie wyłącza dochodzenia przez Zamawiającego roszczeń z tytułu nienależytego wykonania Umowy, w szczególności w przypadku wykrycia wad przedmiotu Umowy przez Zamawiającego po dokonaniu odbioru.
9. Osobami upoważnionymi do udziału w czynnościach odbioru są przedstawiciele Stron wskazani w § 1 ust. 18 Umowy lub inni przedstawiciele stron Umowy.
10. W przypadku wystawiania przez Wykonawcę ustrukturyzowanych faktur elektronicznych w rozumieniu art. 6 ust. 1 ustawy z dnia 9 listopada 2018 r. o elektronicznym fakturowaniu w zamówieniach publicznych, koncesjach na roboty budowlane lub usługi oraz partnerstwie publiczno-prywatnym (t. j. Dz. U. 2020 poz. 1666 ze zm.) za pośrednictwem Platformy Elektronicznego Fakturowania dostępnej pod adresem: https://efaktura.gov.pl/, w polu „referencja", Wykonawca wpisze następujący adres e-mail: iwona.gajda@uj.edu.pl.
11. Wynagrodzenie przysługujące Wykonawcy jest płatne przelewem z rachunku Zamawiającego na konto Wykonawcy wskazane na fakturze.
12. Miejscem płatności jest Bank Zamawiającego, a zaś za datę płatności uznaje się datę zlecenia przelewu przez Zamawiającego.
13. W przypadku faktury korygującej, Wykonawca zobowiązany jest w ciągu 14 dni od daty jej wystawienia dokonać zwrotu środków na rachunek bankowy, z którego nastąpiła zapłata.
14. Wykonawca zobowiązany jest do wskazania na fakturze numeru rachunku, który został ujawniony w wykazie podmiotów zarejestrowanych jako podatnicy VAT, niezarejestrowanych oraz wykreślonych i przywróconych do rejestru VAT prowadzonym przez Szefa Krajowej Administracji Skarbowej (tzw. „Biała lista" – art. 96b ust. 1 ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług – t. j. Dz. U. 2024 poz. 361 ze zm.), zwanej dalej „p.t.u.".
15. W razie braku ujawnienia bankowego rachunku rozliczeniowego Wykonawcy na „Białej liście" Zamawiający będzie uprawniony do zapłaty wynagrodzenia na rachunek wskazany w fakturze Wykonawcy przy zastosowaniu mechanizmu podzielonej płatności albo do zawiadomienia właściwego naczelnika urzędu skarbowego przy dokonywaniu pierwszej zapłaty wynagrodzenia przelewem na rachunek wskazany w tej fakturze.
16. Zamawiający w przypadku, gdy Wykonawca jest zarejestrowany jako czynny podatnik podatku od towarów i usług Zamawiający może dokonać płatności wynagrodzenia z zastosowaniem mechanizmu podzielonej płatności, to jest w sposób wskazany w art. 108a ust. 2 p.t.u. Postanowień zdania 1. nie stosuje się, gdy przedmiot Umowy stanowi czynność zwolnioną z podatku VAT albo jest on objęty 0% stawką podatku VAT.
17. Zamawiający dokona płatności wynagrodzenia przelewem z rachunku Zamawiającego, na rachunek bankowy Wykonawcy wskazany w fakturze, z zastrzeżeniem ust. 15 oraz 16 powyżej.
18. Wykonawca potwierdza, iż ujawniony na fakturze bankowy rachunek rozliczeniowy służy mu dla celów rozliczeń z tytułu prowadzonej przez niego działalności gospodarczej, dla którego prowadzony jest rachunek VAT.
19. Wykonawcy nie przysługuje prawo przenoszenia wierzytelności wynikających z niniejszej Umowy, bez uprzedniej Wykonawca.

§ 5

1. Strony zastrzegają sobie prawo do dochodzenia kar umownych za niezgodne z niniejszą Umową lub nienależyte wykonanie zobowiązań z Umowy wynikających.
2. Wykonawca, z wyjątkiem, gdy postawę naliczenia kar umownych stanowią jego zachowania niezwiązane bezpośrednio lub pośrednio z przedmiotem Umowy lub jej prawidłowym wykonaniem, oraz z zastrzeżeniem ust. 4 niniejszego paragrafu, zapłaci Zamawiającemu karę umowną w poniższej wysokości w przypadku:

2.1. odstąpienie od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy w wysokości 10% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy,
2.2. niewykonania lub nienależytego wykonania Umowy wskutek okoliczności od Zamawiającego niezależnych w wysokości 10% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy,
2.3. zwłoki w uruchomieniu Oprogramowania na stronie internetowej wskazanej w § 1 ust. 17 Umowy, w wysokości 0,5% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy za każdy roboczy dzień zwłoki, licząc od następnego dnia po upływie terminu określonego w § 1 ust. 17 niniejszej Umowy, jednak nie więcej niż 30% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy,
2.4. zwłoki w usunięciu wad Licencji Oprogramowania ujawnionych przy odbiorze, w wysokości 0,5% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy za każdy roboczy dzień zwłoki, licząc od następnego dnia po upływie terminu określonego w § 4 ust. 7 niniejszej Umowy, jednak nie więcej niż 30% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy,
2.5. przerwy w dostępie do Oprogramowania trwającej powyżej 24 godzin w wysokości 0,5% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy za każde rozpoczęte 24 godziny przerwy, jednak nie więcej niż 30% wynagrodzenia brutto wskazanego w § 3 ust. 2 Umowy,

przy czym łączna maksymalna wysokość kar umownych ze wszystkich tytułów wskazanych powyżej nie może przekroczyć 30% wynagrodzenia brutto ustalonego w § 3 ust. 2 Umowy.

3. Zamawiający zapłaci Wykonawcy karę umowną w wysokości 10% wynagrodzenia brutto ustalonego w § 3 ust. 2 Umowy w przypadku odstąpienia od niniejszej Umowy przez Wykonawcę z przyczyn leżących wyłącznie po stronie Zamawiającego, z wyłączeniem okoliczności wskazanej w § 6 ust. 3 oraz 4 Umowy.
4. Zamawiający zastrzega sobie prawo do potrącenia ewentualnych kar umownych z należnej faktury lub innej wymagalnej wierzytelności Wykonawcy, na co wyraża on zgodę.
5. Jeżeli zastrzeżona w niniejszej Umowie kara umowna nie pokrywa poniesionej szkody, Strona, która poniosła szkodę może dochodzić na zasadach ogólnych odszkodowania uzupełniającego, przy czym kary umowne wskazanej w ust. 2 lub 3 powyżej mają charakter zaliczany na poczet ww. odszkodowania.
6. Roszczenie o zapłatę kar umownych staje się wymagalne począwszy od dnia następnego po dniu, w którym miały miejsce okoliczności faktyczne określone w niniejszej Umowie, stanowiące podstawę do ich naliczenia.
7. Uiszczanie kar umownych nie zwalnia Wykonawcy z obowiązku dalszego realizowania zamówienia, zgodnie z postanowieniami niniejszej Umowy.
8. Wykonawcy nie przysługuje odszkodowanie za odstąpienie Zamawiającego od Umowy z przyczyn, za które Zamawiający nie ponosi odpowiedzialności.
9. W przypadku odstąpienia od Umowy, Strony zachowują prawo egzekucji kar umownych.

§ 6

1. Oprócz przypadków wymienionych w Kodeksie cywilnym Stronom przysługuje prawo odstąpienia od niniejszej Umowy w razie zaistnienia okoliczności wskazanej w ust. 2.
2. Zamawiający może odstąpić od Umowy w terminie do 30 dni od dnia powzięcia wiadomości o zaistnieniu jednej z poniższych okoliczności, to jest gdy:
   2.1. Wykonawca na skutek swojej niewypłacalności nie wykonuje zobowiązań pieniężnych przez okres co najmniej 3 miesięcy,
   2.2. zostanie podjęta likwidacja Wykonawcy lub rozwiązanie Wykonawcy bez przeprowadzenia likwidacji, bądź nastąpi zakończenie prowadzenia działalności gospodarczej przez Wykonawcę bądź wykreślenie Wykonawcy jako przedsiębiorcy z CEIDG albo śmierć Wykonawcy będącego osobą fizyczną,
   2.3. został wydany nakaz zajęcia majątku Wykonawcy w stopniu uniemożliwiającym należyte wykonanie przedmiotu zamówienia,
   2.4. wystąpiły u Wykonawcy duże trudności finansowe, w szczególności wystąpiły zajęcia dokonane przez uprawnione organy na postawie powszechnie obowiązujących przepisów prawa o łącznej wartości przekraczającej 100 000,00 PLN (słownie: sto tysięcy złotych $^{00}/_{100}$),
   2.5. dostarczył/uruchomił przedmiot Umowy lub świadczył usługę niezgodnie z warunkami Umowy

lub przekroczył terminu realizacji Umowy o 7 dni, bez konieczności wskazania przez Zamawiającego dodatkowego terminu dostawy.

3. Zamawiającemu przysługuje także prawo odstąpienia od niniejszej Umowy w terminie 12 miesięcy liczonym od dnia, w którym Zamawiający dowiedział się o istnieniu wady prawnej Oprogramowania, a jeżeli dowiedział się on o istnieniu wady dopiero na skutek powództwa osoby trzeciej – od dnia, w którym orzeczenie wydane w sporze z osobą trzecią stało się prawomocne.
4. Zamawiający, niezależnie od postanowień ust. 2 i 3 niniejszego paragrafu Umowy, w razie wystąpienia poniżej wskazanych okoliczności:
   4.1. w terminie 30 dni od dnia powzięcia wiadomości o zaistnieniu istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, czego nie można było przewidzieć w chwili zawarcia Umowy, lub dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu (art. 456 ust. 1 pkt 1 PZP),
   4.2. gdy dokonano zmiany Umowy z naruszeniem art 454 i art. 455 PZP,
   4.3. Wykonawca w chwili zawarcia Umowy podlegał wykluczeniu z postępowania na podstawie okoliczności wskazanych Rozdziale VII SWZ,
   4.4. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, w ramach procedury przewidzianej w art. 258 Traktatu o funkcjonowaniu Unii Europejskiej, że Rzeczpospolita Polska uchybiła zobowiązaniom, które ciążą na niej na mocy Traktatów, dyrektywy 2014/24/UE, dyrektywy 2014/25/UE i dyrektywy 2009/81/WE, z uwagi na to, że Zamawiający udzielił zamówienia z naruszeniem prawa Unii Europejskiej.
5. W przypadku odstąpienia od Umowy przez Zamawiającego z przyczyn leżących po stronie Wykonawcy oraz w razie zaistnienia okoliczności wskazanych w ust. 4 powyżej, Wykonawca może żądać wynagrodzenia tylko za wykonaną część przedmiotu zamówienia.
6. Zamawiający, korzystając z umownego lub ustawowego prawa odstąpienia od Umowy może odstąpić – zgodnie ze swoim wyborem – od całości Umowy lub od jej części.
7. Wykonawcy nie przysługuje kara umowna lub odszkodowanie z tytułu odstąpienia przez Zamawiającego od Umowy z powodu okoliczności leżących po stronie Wykonawcy lub na podstawie ust. 2, 3 lub 4 powyżej.
8. Odstąpienie od Umowy powinno nastąpić w formie pisemnej pod rygorem nieważności takiego oświadczenia i powinno zawierać uzasadnienie.
9. Odstąpienie od Umowy nie wpływa na istnienie i skuteczność roszczeń o zapłatę kar umownych.

§ 7

1. Przez siłę wyższą, rozumie się zdarzenie niezależne od Wykonawcy, nie wynikające z jego i jego podwykonawców problemów organizacyjnych, którego wystąpienia lub skutków nie mógł przewidzieć lub któremu nie mógł zapobiec, ani któremu nie mógł przeciwdziałać, a które uniemożliwiają Wykonawcy wykonanie w części lub w całości jego zobowiązania wynikającego z niniejszej Umowy albo mającej bezpośredni wpływ na terminowość i sposób wykonywanych Umowy. Strony za okoliczności siły wyższej uznają w szczególności: ogłoszone stany klęski żywiołowej, w tym powódź i trzęsienie ziemi, upadek statku powietrznego, strajki generalne lub lokalne, działania wojenne lub ogłoszenie stanu wojennego, atak terrorystyczny, ogłoszone stany wyjątkowe, ogłoszenie stanu zagrożenia epidemicznego albo ogłoszenie stanu epidemii, w tym epidemii choroby zagrażającej zdrowiu lub życiu wielu osób.
2. Jeżeli wskutek okoliczności siły wyższej Strona nie będzie mogła wykonywać swoich obowiązków umownych w całości lub w części, niezwłocznie powiadomi o tym drugą stronę. W takim przypadku Strony uzgodnią sposób i zasady dalszego wykonywania Umowy, czasowo zawieszą jej realizację lub Umowa zostanie rozwiązana.
3. Bieg terminów określonych w niniejszej Umowie ulega zawieszeniu przez czas trwania przeszkody spowodowanej siłą wyższą.

§ 8

1. Wszelkie oświadczenia Stron Umowy będą składane w formie pisemnej pod rygorem nieważności listem poleconym lub za potwierdzeniem ich złożenia.
2. Strony zobowiązują się do każdorazowego powiadamiania listem poleconym o zmianie adresu swojej siedziby, pod rygorem uznania za skutecznie doręczoną korespondencję wysłaną pod dotychczas znany adres.
3. Ewentualna nieważność jednego lub kilku postanowień niniejszej Umowy nie wpływa na ważność Umowy w całości, a w takim przypadku Strony zastępują nieważne postanowienie postanowieniem zgodnym z celem i innymi postanowieniami Umowy, z zastrzeżeniem zdania 2. Zmiany Umowy dokonane niezgodnie z postanowienia § 9 ust. 1 lub 2 niniejszej Umowy podlegają unieważnieniu, w takim przypadku w miejsce unieważnionych zmodyfikowanych postanowień Umowy stosuje się postanowienia umowne w ich pierwotnym brzmieniu.

§ 9

1. Strony dopuszczają możliwość zmiany Umowy po uprzednim sporządzeniu protokołu konieczności, przy zachowaniu wynagrodzenia Wykonawcy wskazanego w § 3 ust. 2 Umowy, poprzez podpisanie aneksu do Umowy, w przypadku zaistnienia okoliczności wskazanych w treści art. 455 ust. 1 pkt 2 – 4 oraz art. 455 ust. 2 ustawy PZP, oraz w poniżej wskazanych przypadkach:
   1.1. zmiany terminu realizacji zamówienia (aktywacji wszystkich lub pojedynczego suportu lub okresu trwania całej asysty technicznej), poprzez jego przedłużenie ze względu na przyczyny leżące po stronie Zamawiającego dotyczące np. braku przygotowania/przekazania miejsca realizacji/dostawy, oraz inne niezawinione przez Strony przyczyny, w tym spowodowane przez tzw. siłę wyższą w rozumieniu § 8 Umowy;
   1.2. zmiany określonego typu, modelu, nazwy, producenta przedmiotu Umowy bądź jego elementów, poprawy jakości lub innych parametrów charakterystycznych dla danego elementu dostawy lub zmiany technologii na równoważną lub lepszą w szczególności w przypadku zakończenia jego produkcji lub wstrzymania lub wycofania go z produkcji po przedstawianiu stosownych dokumentów od producenta lub dystrybutora, z tym że cena wskazana w § 3 ust. 2 Umowy nie może ulec podwyższeniu, a parametry techniczne nie mogą być gorsze niż wskazane w treści oferty,
   1.3. aktualizacji rozwiązań z uwagi na postęp technologiczny lub zmiany obowiązujących przepisów,
   1.4. zmiany podwykonawcy, w szczególności ze względów losowych lub innych korzystnych dla Zamawiającego.
2. Ponadto dopuszcza się zastąpienie dotychczasowego Wykonawcy niniejszej Umowy przez inny podmiot spełniający warunki udziału w postępowaniu oraz niepodlegający wykluczeniu z postępowania na mocy art. 108 ust. 1 ustawy PZP i art. 109 ust. 1 ustawy PZP w zakresie wskazanym w dokumentach postępowania przez Zamawiającego, w razie gdy nastąpiło połączenie, podział, przekształcenie, upadłość, restrukturyzacja, nabycie dotychczasowego Wykonawcy lub nabycie jego przedsiębiorstwa przez ww. podmiot.
3. Niezależnie od postanowień ust. 1 i 2 powyżej, Strony Umowy mogą dokonywać nieistotnych zmian Umowy, niestanowiących istotnej zmiany Umowy w rozumieniu art. 454 ust. 2 ustawy PZP, poprzez zawarcie pisemnego aneksu pod rygorem nieważności.
4. Zmiana wynagrodzenia Wykonawcy wchodzi w życie z dniem zawarcia aneksu, nastąpi od daty wprowadzenia zmiany w Umowie i dotyczy wyłącznie niezrealizowanej części Umowy.
5. Strona występująca o zmianę postanowień niniejszej Umowy zobowiązana jest do udokumentowania zaistnienia okoliczności, o których mowa w ust. 1 lub 2 powyżej. Wniosek o zmianę postanowień niniejszej Umowy musi być wyrażony w formie pisemnej na zasadach wskazanych w art. 78 lub 78^1 Kodeksu cywilnego.
6. Zmiany niedotyczące postanowień umownych np. gdy z przyczyn organizacyjnych skutkujące koniecznością zmiany danych teleadresowych określonych w Umowie, w szczególności zmiana numeru konta bankowego jednej ze Stron, nie wymagają zawarcia pisemnego aneksu do Umowy, dlatego nastąpią poprzez przekazanie pisemnego oświadczenie Strony, której te zmiany dotyczą, drugiej Stronie.

§ 10

1. Strony zgodnie postanawiają, że informacje, dane i dokumenty przekazane Wykonawcy przez Zamawiającego oraz Zamawiającemu przez Wykonawcę w ramach niniejszej Umowy i oznaczone klauzulą przy przekazaniu w formie pisemnej jako „Informacja Poufna", stanowią informacje poufne (zwane dalej „Informacjami Poufnymi"). Wykonawca zobowiązuje się do zachowania w bezwzględnej tajemnicy wszelkich Informacji Poufnych dotyczących Zamawiającego, w szczególności ma zakaz ich ujawniania osobom trzecim w jakiejkolwiek formie. Powyższy zakaz pozostaje w mocy również po wygaśnięciu Umowy przez okres 3 (trzech) lat od daty wygaśnięcia Umowy.
2. Zakazu, o którym mowa w ust. 1, nie stosuje się do informacji:
   2.1. podlegających ujawnieniu organowi państwowemu, właściwemu sądowi lub innemu podmiotowi zgodnie z powszechnie obowiązującymi przepisami prawa;
   2.2. uzgodnionych na piśmie pomiędzy Stronami jako podlegające ujawnieniu.
3. Odpowiednio Wykonawca i Zamawiający mają zakaz wykorzystywania Informacji Poufnych Zamawiającego i Wykonawcy zgromadzonych w związku z realizacją Umowy w jakichkolwiek innych celach oraz w jakikolwiek inny sposób, aniżeli w celu i w związku z realizacją Umowy.
4. Strony mają zakaz udostępniania zgromadzonych Informacji Poufnych drugiej Strony lub danych osobowych pracowników jakimkolwiek osobom trzecim, chyba że uzyskają na to pisemną zgodę drugiej Strony, z zastrzeżeniem ust. 2 powyżej.

§ 11

1. Żadna ze Stron nie jest uprawniona do przeniesienia swoich praw i zobowiązań z tytułu niniejszej Umowy bez uzyskania pisemnej zgody drugiej Strony, w szczególności Wykonawcy nie przysługuje prawo przenoszenia wierzytelności wynikających z niniejszej Umowy bez uprzedniej pisemnej zgody Zamawiającego.
2. Strony zobowiązują się do każdorazowego powiadamiania listem poleconym o zmianie adresu swojej siedziby, pod rygorem uznania za skutecznie doręczoną korespondencję wysłaną pod dotychczas znany adres.
3. Wszelkie zmiany lub uzupełnienia niniejszej Umowy mogą nastąpić za zgodą Stron w formie pisemnego aneksu pod rygorem nieważności.
4. W sprawach nieuregulowanych niniejszą Umową mają zastosowanie przepisy ustawy z dnia 11 września 2019 r. – Prawo zamówień publicznych (t. j. Dz. U. 2023 poz. 1605 ze zm.), ustawy z dnia 2 marca 2020 r. o szczególnych rozwiązaniach związanych z zapobieganiem, przeciwdziałaniem i zwalczaniem COVID-19, innych chorób zakaźnych oraz wywołanych nimi sytuacji kryzysowych (t. j. Dz. U. 2024 poz. 340 ze zm.) oraz ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t. j. Dz. U. 2023 poz. 1610 ze zm.).
5. W przypadku zaistnienia pomiędzy stronami sporu, wynikającego z Umowy lub pozostającego w związku z Umową, strony zobowiązują się do podjęcia próby jego rozwiązania w drodze mediacji prowadzonej przez Mediatorów Stałych Sądu Polubownego przy Prokuratorii Generalnej RP, zgodnie z Regulaminem tego Sądu, a dopiero w przypadku braku zawarcia ugody przed Mediatorem Stałym Sądu Polubownego przy Prokuratorii Generalnej RP, spór będzie poddany rozstrzygnięciu przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
6. Umowa niniejsza została sporządzona pisemnie na zasadach określonych w art. 78 i 78^1 Kodeksu cywilnego tj. opatrzona przez upoważnionych przedstawicieli obu Stron podpisami kwalifikowanymi lub podpisami własnoręcznymi w dwóch (2) jednobrzmiących egzemplarzach, po jednym (1) dla każdej ze Stron, z zastrzeżeniem ust. 7 poniżej.
7. Strony zgodnie oświadczają, że w przypadku zawarcia niniejszej Umowy w formie elektronicznej za pomocą kwalifikowanego podpisu elektronicznego, będącej zgodnie z art. 78^1 KC równoważną w stosunku do zwykłej formy pisemnej. Powstały w ten sposób dokument elektroniczny stanowi poświadczenie, iż Strony zgodnie złożyły oświadczenia woli w nim zawarte, zaś datą zawarcia jest dzień złożenia ostatniego (późniejszego) oświadczenia woli o jej zawarciu przez umocowanych przedstawicieli każdej ze Stron.

Załącznik do Umowy stanowi:
2. Wzór protokołu odbioru.

.....	.....
Zamawiający	*Wykonawca*

Załącznik nr 2 do Umowy nr 80.272.206.2024

…….
pieczątka Jednostki UJ

Protokół odbioru

W dniu ……. r. w związku z Umową nr 80.272.206.2024 z dnia ……. r.

DOKONANO / NIE DOKONANO* odbioru:

Dane dostawcy …….

Lp. Nazwa oprogramowania

Zgodnie z Umową odbiór powinien nastąpić do dnia .....

Odbiór został wykonany w terminie/nie został wykonany w terminie*

BEZ UWAG I ZASTRZEŻEŃ / UWAGI I ZASTRZEŻENIA*

……
……
……
……
……
……..……
……

podpis osoby odbierającej

w imieniu Zamawiającego W imieniu Wykonawcy

*Niepotrzebne skreślić

Załącznik A do SWZ

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA – SPECYFIKACJA TECHNICZNA

Wymagania ogólne

1. Oferowane rozwiązanie musiało brać udział w teście skuteczności ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla nie wcześniej niż w 2023 roku i uzyskać mniej niż 25% braku wykryć (none detections).

Ochrona stacji roboczych – Windows

2. Rozwiązanie musi wspierać systemy Windows 10/Windows 11.
3. Rozwiązanie musi wspierać architekturę 32 i 64-bitową systemu Windows.
4. Rozwiązanie musi wspierać architekturę ARM64.
5. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
6. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
7. Pomoc w rozwiązaniu (help) i dokumentacja rozwiązania dostępna co najmniej w języku polskim oraz angielskim.
8. Skuteczność rozwiązania potwierdzona nagrodami VB100 i AVcomparatives.

Ochrona antywirusowa i antyspyware

9. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
10. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
11. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
12. Rozwiązanie musi integrować się z Intel Threat Detection Technology.
13. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
14. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
15. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
16. Rozwiązanie musi posiadać możliwość definiowania zadań w harmonogramie, w taki sposób, aby zadanie przed wykonaniem sprawdzało czy komputer pracuje na zasilaniu bateryjnym, jeśli tak – nie wykonywało danego zadania.
17. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: co godzinę, po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (czyli metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania, priorytet skanowania).
18. Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
19. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
20. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.

21. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
22. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
23. Administrator musi mieć możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
24. Rozwiązanie musi posiadać możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.
25. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
26. Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera.
27. W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji.
28. Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.
29. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
30. Rozwiązanie musi posiadać wbudowany konektor dla programu Microsoft Outlook.
31. Rozwiązanie musi umożliwiać skanowanie i oczyszczanie w czasie rzeczywistym poczty przychodzącej i wychodzącej obsługiwanej przy pomocy programu Microsoft Outlook.
32. 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).
33. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
34. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
35. Rozwiązanie musi umożliwiać skanowanie ruchu HTTP na poziomie stacji roboczych. Zainfekowany ruch jest automatycznie blokowany, a użytkownikowi wyświetlane jest stosowne powiadomienie.
36. Rozwiązanie musi posiadać możliwość blokowania możliwości przeglądania wybranych stron internetowych. Rozwiązanie musi umożliwić blokowanie danej strony internetowej po podaniu przynajmniej całego adresu URL strony lub części adresu URL.
37. Rozwiązanie musi posiadać możliwość zdefiniowania blokady wszystkich stron internetowych z wyjątkiem listy stron, ustalonej przez administratora.
38. Rozwiązanie musi automatycznie integrować się z dowolną przeglądarką internetową bez konieczności zmian w konfiguracji.
39. Rozwiązanie musi umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.
40. Rozwiązanie musi zapewniać skanowanie ruchu szyfrowanego transparentnie bez potrzeby konfiguracji zewnętrznych aplikacji, takich jak: przeglądarki internetowe oraz programy pocztowe.
41. Rozwiązanie musi posiadać możliwość zgłoszenia witryny z podejrzeniem phishingu z poziomu graficznego interfejsu użytkownika, w celu analizy przez laboratorium producenta.
42. Administrator ma mieć możliwość zdefiniowania portów TCP, na których rozwiązanie będzie realizowało proces skanowania ruchu szyfrowanego.
43. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.

44. Procesy zweryfikowane jako bezpieczne mają być pomijane podczas procesu skanowania oraz przez moduły ochrony w czasie rzeczywistym.
45. Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.
46. W przypadku, gdy stacja robocza nie będzie posiadała dostępu do sieci Internet, ma odbywać się skanowanie wszystkich procesów, również tych, które wcześniej zostały uznane za bezpieczne.
47. Rozwiązanie musi posiadać dwa wbudowane 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.
48. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
49. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
50. Do wysłania próbki zagrożenia do laboratorium producenta, rozwiązanie nie może wykorzystywać klienta pocztowego zainstalowanego na komputerze użytkownika.
51. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
52. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
53. Rozwiązanie musi posiadać możliwość zabezpieczenia przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora. Przy próbie deinstalacji rozwiązanie musi pytać o hasło.
54. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
55. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku aktualizacji – poinformować o tym użytkownika i wyświetlenia listy niezainstalowanych aktualizacji.
56. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
57. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
58. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
59. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
60. Rozwiązanie musi posiadać umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth, czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
61. Funkcja blokowania nośników wymiennych, bądź grup urządzeń, ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń, minimum w oparciu o typ, numer seryjny, dostawcę oraz model urządzenia.

62. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
63. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
64. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
65. W momencie podłączenia zewnętrznego nośnika, rozwiązanie musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
66. Administrator ma posiadać możliwość takiej konfiguracji rozwiązania, aby skanowanie całego nośnika odbywało się automatycznie lub za potwierdzeniem przez użytkownika.
67. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
68. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. 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,
    e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o szczególnie podejrzanych zdarzeniach.
69. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
70. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
71. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
72. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
73. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której zostało zainstalowane, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
74. 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.
75. Rozwiązanie musi posiadać funkcję, która aktywnie monitoruje wszystkie pliki programu, jego procesy, usługi i wpisy w rejestrze i skutecznie blokuje ich modyfikacje przez aplikacje trzecie.
76. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
77. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
78. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po

upływie którego rozwiązanie zgłosi posiadanie nieaktualnego silnika detekcji.

79. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
80. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
81. Rozwiązanie musi być wyposażone w funkcjonalność, umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
82. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
83. Rozwiązanie musi posiadać funkcjonalność, która automatycznie wykrywa aplikacje pracujące w trybie pełnoekranowym.
84. W momencie wykrycia trybu pełnoekranowego, rozwiązanie ma wstrzymać wyświetlanie wszystkich powiadomień związanych ze swoją pracą oraz wstrzymać zadania znajdujące się w harmonogramie zadań rozwiązania.
85. Użytkownik ma mieć możliwość skonfigurowania po jakim czasie włączone mają zostać powiadomienia oraz zadania, pomimo pracy w trybie pełnoekranowym.
86. Rozwiązanie musi być wyposażone w dziennik zdarzeń, rejestrujący informacje na temat znalezionych zagrożeń, kontroli dostępu do urządzeń, skanowania oraz zdarzeń.
87. Rozwiązanie musi posiadać możliwość utworzenia dziennika diagnostycznego z poziomu interfejsu aplikacji.
88. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji programu w trybie offline.
89. Rozwiązanie musi mieć możliwość podejrzenia informacji o licencji, która znajduje się w programie.
90. W trakcie instalacji rozwiązanie ma umożliwiać wybór komponentów, które mają być instalowane. Instalator ma zezwalać na wybór co najmniej następujących modułów do instalacji: kontrola dostępu do urządzeń, zapora osobista, ochrona poczty, ochrona protokołów, kontrola dostępu do stron internetowych, RMM.
91. W rozwiązaniu musi istnieć możliwość tymczasowego wstrzymania działania polityk, wysłanych z poziomu serwera zdalnej administracji.
92. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień rozwiązania na stacji końcowej.
93. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostaną przywrócone dotychczasowe ustawienia.
94. Administrator ma możliwość wstrzymania polityk na 10 minut, 30 minut, 1 godzinę lub 4 godziny.
95. Aktywacja funkcji wstrzymania polityki musi obsługiwać uwierzytelnienie za pomocą hasła lub konta użytkownika.
96. Rozwiązanie musi posiadać opcję automatycznego skanowania komputera po wyłączeniu wstrzymania polityki.
97. Rozwiązanie musi posiadać możliwość zmiany konfiguracji programu z poziomu dedykowanego modułu wiersza poleceń. Zmiana konfiguracji jest w takim przypadku autoryzowana bez hasła lub za pomocą hasła do ustawień zaawansowanych.
98. Rozwiązanie musi posiadać możliwość definiowana stanów rozwiązania, jakie będą wyświetlane użytkownikowi, co najmniej: ostrzeżeń o wyłączonych mechanizmach ochrony czy stanie licencji.
99. Administrator musi mieć możliwość dodania własnego komunikatu do stopki powiadomień, jakie będą wyświetlane użytkownikowi na pulpicie.
100. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez

wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.

101. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika, aż do momentu wykrycia zagrożenia.
102. Rozwiązanie musi posiadać dedykowany moduł, zapewniający ochronę przed oprogramowaniem wymuszającym okup.
103. Administrator ma możliwość dodania wykluczenia dla procesu, wskazując plik wykonywalny.
104. Rozwiązanie musi posiadać możliwość przeskanowania pojedynczego pliku, poprzez opcję „przeciągnij i upuść"
105. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
106. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
107. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
108. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
109. Rozwiązanie musi posiadać ochronę przed dołączeniem komputera do sieci botnet.
110. Rozwiązanie musi posiadać ochronę przed atakami Brute-Force, która zablokuje próbę siłowego dostania się do stacji roboczej za pomocą protokołu RDP i SMB.
111. Rozwiązanie musi posiadać pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
112. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora, autoryzowanego przez producenta programu.

Ochrona przed spamem

113. Rozwiązanie musi posiadać ochronę antyspamową dla programu pocztowego Microsoft Outlook.
114. Rozwiązanie musi umożliwiać wyłączenie skanowania baz programu pocztowego po zmianie zawartości skrzynki odbiorczej.
115. Rozwiązanie musi umożliwiać automatyczne wpisanie do białej listy wszystkich kontaktów z książki adresowej programu pocztowego.
116. Rozwiązanie musi posiadać możliwość ręcznej zmiany klasyfikacji wiadomości spamu na pożądaną lub niepożądaną bezpośrednio z klienta pocztowego.
117. Rozwiązanie musi posiadać możliwość ręcznego dodania nadawcy wiadomości do białej lub czarnej listy bezpośrednio z klienta pocztowego.
118. Rozwiązanie musi posiadać możliwość definiowania folderu, gdzie program pocztowy będzie umieszczać spam.
119. Rozwiązanie musi możliwość zdefiniowania dowolnego tekstu, dodawanego do tematu wiadomości zakwalifikowanej jako spam.
120. Rozwiązanie musi domyślnie współpracować z folderem „Wiadomości-śmieci", dostępnym w programie Microsoft Outlook.
121. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości typu spam na pożądaną, oznaczy ją jako „nieprzeczytana"
122. Rozwiązanie ma umożliwiać funkcjonalność, która po zmianie klasyfikacji wiadomości pożądanej na spam oznaczy ją jako „przeczytana".
123. Rozwiązanie musi posiadać funkcjonalność wyłączenia modułu antyspamowego na określony czas lub do czasu ponownego uruchomienia komputera.

Zapora osobista (personal firewall)

124. Zapora osobista rozwiązania musi pracować w jednym z czterech trybów:
    a. tryb automatyczny – rozwiązanie blokuje cały ruch przychodzący i zezwala tylko na połączenia wychodzące,
    b. tryb interaktywny – rozwiązanie pyta się o każde nowo nawiązywane połączenie,
    c. tryb oparty na regułach – rozwiązanie blokuje cały ruch przychodzący i wychodzący, zezwalając tylko na połączenia skonfigurowane przez administratora,
    d. tryb uczenia się – rozwiązanie automatycznie tworzy nowe reguły zezwalające na połączenia przychodzące i wychodzące. Administrator musi posiadać możliwość konfigurowania czasu działania trybu.
125. Rozwiązanie musi oceniać reguły zapory systemu Windows.
126. Rozwiązanie musi posiadać możliwość tworzenia list sieci zaufanych.
127. Rozwiązanie musi posiadać możliwość dezaktywacji funkcji zapory sieciowej poprzez trwałe wyłączenie.
128. Rozwiązanie musi posiadać możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji, usługi i adresu lub zakresu adresów komputera lokalnego lub/i zdalnego.
129. Rozwiązanie musi posiadać możliwość wyboru jednej z trzech akcji w trakcie tworzenia reguł w trybie interaktywnym: zezwól, zablokuj i pytaj.
130. Rozwiązanie musi posiadać możliwość powiadomienia użytkownika o nawiązaniu określonych połączeń oraz odnotowanie faktu nawiązania danego połączenia w dzienniku zdarzeń aplikacji.
131. Rozwiązanie musi posiadać możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer, w tym minimum dla strefy zaufanej i sieci Internet.
132. Rozwiązanie musi wykrywać modyfikację w aplikacjach, korzystających z sieci i powiadamianie o tym zdarzeniu.
133. Rozwiązanie musi posiadać możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
134. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci.
135. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
136. Autoryzacja stref ma się odbywać min. w oparciu o: zaaplikowany profil połączenia, adres serwera DNS, sufiks domeny, adres domyślnej bramy, adres serwera WINS, adres serwera DHCP, lokalny adres IP, identyfikator SSID, szyfrowania sieci bezprzewodowej lub jego brak, konkretny interfejs sieciowy w systemie.
137. Podczas konfiguracji autoryzacji sieci, administrator ma mieć możliwość definiowania adresów IP dla lokalnego połączenia, adresu IP serwera DHCP, adresu serwera DNS oraz adresu IP serwera WINS, zarówno z wykorzystaniem adresów IPv4 jak i IPv6.
138. Opcje związane z autoryzacją stref mają posiadać możliwość łączenia (np. lokalnego adresu IP z adresem serwera DNS) w dowolnej kombinacji, celem zwiększenia dokładności identyfikacji danej sieci.
139. Rozwiązanie musi posiadać kreator, który umożliwia rozwiązywanie problemów z połączeniem. Musi pozwalać na rozwiązanie problemów:
    a. z aplikacją lokalną, którą administrator wskazuje z listy,
    b. z połączeniem z urządzeniem zdalnym, na podstawie jego adresuIP.

Kontrola dostępu do stron internetowych

140. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli dostępu do stron internetowych.
141. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość utworzenia reguł w oparciu o użytkownika lub grupę użytkowników systemu Windows lub Active Directory.
142. Rozwiązanie musi posiadać możliwość filtrowania adresów URL w oparciu o co najmniej 140 kategorii i podkategorii.
143. Podstawowe kategorie, w jakie rozwiązanie musi być wyposażone to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
144. Moduł musi posiadać możliwość grupowania kategorii oraz adresów stron internetowych.
145. Lista adresów URL znajdujących się w poszczególnych kategoriach, musi być automatycznie aktualizowana przez producenta.
146. Administrator musi posiadać możliwość wyłączenia integracji modułu kontroli dostępu do stron internetowych.
147. Rozwiązanie musi posiadać możliwość określenia przynajmniej jednej z akcji dla reguły kontroli dostępu do stron internetowych: zezwól, ostrzeż, blokuj.
148. Rozwiązanie musi posiadać także możliwość dodania komunikatu i grafiki w przypadku zablokowania, określonej w regułach, strony internetowej.

Bezpieczna przeglądarka

149. Rozwiązanie musi być wyposażona w moduł bezpiecznej przeglądarki.
150. Przeglądarka musi automatycznie szyfrować wszelkie dane wprowadzane przez Użytkownika.
151. Użytkownik w momencie wejścia na stronę, która znajduje się na liście chronionych witryn, musi automatycznie zostać przekierowany do okna bezpiecznej przeglądarki.
152. Administrator musi mieć możliwość konfiguracji listy chronionych witryn, przez bezpieczną przeglądarkę.
153. Administrator musi mieć możliwość konfiguracji, aby użytkownik przy próbie dostępu do strony bankowości elektronicznej, automatycznie został przekierowany do okna bezpiecznej przeglądarki.
154. Praca w bezpiecznej przeglądarce musi być wyróżniona poprzez odpowiedni kolor ramki przeglądarki oraz informację na ramce przeglądarki.

Ochrona stacji roboczych – macOS

1. Rozwiązanie musi posiadać pełne wsparcie dla systemów macOS 10.12 lub nowszych.
2. Rozwiązanie musi wspierać architekturę Apple Silicon (ARM)
3. Rozwiązanie musi być dostępne co najmniej w języku polskim oraz angielskim.
4. Pomoc w rozwiązaniu (help) musi być dostępna co najmniej w języku polskim oraz angielskim.
5. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
6. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.

7. Rozwiązanie musi posiadać funkcjonalność, która w momencie wykrycia trybu pełnoekranowego ma wstrzymać wyświetlanie wszelkich powiadomień związanych ze swoją pracą oraz wstrzymać swoje zadania znajdujące się w harmonogramie zadań.
8. Rozwiązanie musi posiadać możliwość skanowanie w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
9. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.
10. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (np.: co godzinę, po zalogowaniu, po uruchomieniu komputera). Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności).
    Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
11. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
12. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
13. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
14. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.
15. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne (heurystyka) i drugi wykorzystujący aktywne metody heurystyczne oraz elementy sztucznej inteligencji (zaawansowana heurystyka). Musi istnieć możliwość wyboru, z jaką heurystyka ma odbywać się skanowanie – z użyciem jednej i/lub obu metod jednocześnie.
16. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń (wykrytych przez metody heurystyczne) do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie mają być wysyłane automatycznie, oraz czy próbki zagrożeń będą wysyłane w pełni automatycznie czy też po dodatkowym potwierdzeniu przez użytkownika.
17. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
18. Rozwiązanie musi posiadać możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
19. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing”.
20. Rozwiązanie musi posiadać funkcję blokowania nośników wymiennych. Funkcja musi umożliwiać wyłączenie dostępu do nośników: Płyta CD/DVD, Pamięć masowa, karty sieciowe, Drukarka USB, Urządzenie do tworzenia obrazów, Port szeregowy, Urządzenie przenośne.
    Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
21. Aktualizacja silnika detekcji rozwiązania musi być dostępna z Internetu, lokalnego zasobu sieciowego lub przy pomocy serwera HTTP.
22. Rozwiązanie musi posiadać możliwość pobierania aktualizacji za pośrednictwem serwera proxy.
23. Rozwiązanie musi umożliwiać automatyczne sprawdzanie plików wykonywanych podczas uruchamiania systemu operacyjnego.
24. Rozwiązanie musi być wyposażone tylko w jeden skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).

25. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji silnika detekcji i samego oprogramowania oraz dokonanym skanowaniu komputera.
26. Rozwiązanie musi umożliwiać importowanie oraz eksportowanie ustawień. Z poziomu interfejsu graficznego użytkownik ma mieć możliwość przywrócenia wartości domyślnych wszystkich ustawień.
27. Rozwiązanie musi posiadać mechanizm Ochrony dostępu do stron internetowych monitoruje komunikację w ramach protokołu HTTP.
28. Rozwiązanie musi pozwalać na konfigurację portów, dla których ma się odbywać skanowanie protokołu HTTP.
29. Rozwiązanie musi umożliwiać w ramach zdefiniowanej grupy „Uprzywilejowani użytkownicy" na modyfikację konfiguracji programu.
30. Rozwiązanie musi posiadać możliwość zdalnego zarządzania z poziomu Administracji zdalnej.
31. 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).
32. Rozwiązanie musi automatycznie integrować skaner POP3 i IMAP z dowolnym klientem pocztowym bez konieczności zmian w konfiguracji.
33. Rozwiązanie musi umożliwiać definiowanie różnych portów dla POP3 i IMAP, na których ma odbywać się skanowanie.
34. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji w temacie zainfekowanej wiadomości o jej przeskanowaniu.
35. Rozwiązanie musi posiadać możliwość opcjonalnego dołączenia informacji o przeskanowaniu do każdej odbieranej wiadomości e-mail lub tylko do zainfekowanych wiadomości e-mail.
36. Wsparcie techniczne dla rozwiązania musi być świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
37. Zapora osobista rozwiązania musi pracować w jednym z 2 trybów:
    a. Automatyczny z wyjątkami - umożliwia administratorowi zdefiniowanie wyjątków dla ruchu przychodzącego i wychodzącego w liście reguł,
    b. Interaktywny – dla każdej nieznanej komunikacji generowane jest pytanie dla użytkownika o jej odblokowanie.
38. Rozwiązanie musi mieć możliwość określenia w regułach zapory osobistej kierunku ruchu, portu lub zakresu portów, protokołu, aplikacji i adresu komputera zdalnego.
39. Rozwiązanie musi mieć możliwość odnotowania faktu nawiązania danego połączenia w dzienniku zdarzeń.
40. Rozwiązanie musi mieć możliwość zapisywania w dzienniku zdarzeń związanych z zezwoleniem lub zablokowaniem danego typu ruchu.
41. Rozwiązanie musi mieć możliwość zdefiniowania wielu niezależnych zestawów reguł dla każdej sieci, w której pracuje komputer w tym minimum dla profilu: Publiczny, Praca, Dom.
42. Rozwiązanie musi oferować pełne wsparcie zarówno dla protokołu IPv4 jak i dla standardu IPv6.
43. Rozwiązanie musi mieć możliwość tworzenia profili pracy zapory osobistej w zależności od wykrytej sieci.
44. Administrator ma możliwość sprecyzowania, który profil zapory ma zostać zaaplikowany po wykryciu danej sieci. Profile mają możliwość automatycznego przełączania, bez ingerencji użytkownika lub administratora.
45. Aktywacja stref ma się odbywać min. w oparciu o: interfejs sieciowy w systemie, Sieć WiFi, Podsieć IPv4/IPv6, Zakres adresów IPv4/IPv6, Adres IPv4/IPv6.

Kontrola dostępu do stron internetowych:

46. Rozwiązanie musi być wyposażone w zintegrowany moduł kontroli odwiedzanych stron internetowych.
47. Moduł kontroli dostępu do stron internetowych musi posiadać możliwość dodawania różnych użytkowników, dla których będą stosowane zdefiniowane reguły.
48. Dodawanie użytkowników musi być możliwe w oparciu o już istniejące konta użytkowników systemu operacyjnego.
49. Reguły mają być automatycznie aktywowane w zależności od zalogowanego użytkownika.
50. Rozwiązanie musi posiadać możliwość filtrowania URL w oparciu o co najmniej 140 kategorii i podkategorii.
51. Podstawowe kategorie w jakie rozwiązanie musi być wyposażona to: materiały dla dorosłych, usługi biznesowe, komunikacja i sieci społecznościowe, działalność przestępcza, oświata, rozrywka, gry, zdrowie, informatyka, styl życia, aktualności, polityka, religia i prawo, wyszukiwarki, bezpieczeństwo i szkodliwe oprogramowanie, zakupy, hazard, udostępnianie plików, zainteresowania dzieci, serwery proxy, alkohol i tytoń, szukanie pracy, nieruchomości, finanse i pieniądze, niebezpieczne sporty, nierozpoznane kategorie oraz elementy niezaliczone do żadnej kategorii.
52. Lista adresów URL, znajdujących się w poszczególnych kategoriach, musi być na bieżąco aktualizowana przez producenta.
53. Użytkownik musi posiadać możliwość wyłączenia modułu kontroli dostępu do stron internetowych.

Ochrona urządzeń mobilnych opartych o system Android

1. Rozwiązanie musi wspierać system co najmniej Android 6.0.
2. Rozwiązanie musi wspierać rozdzielczość wyświetlacza urządzenia 480x800px lub wyższa.
3. Rozwiązanie musi wspierać procesory: ARM z obsługą ARMv7 lub x86 Intel Atom.
4. Rozwiązanie musi posiadać ochronę plików w czasie rzeczywistym.
5. Rozwiązanie musi posiadać ochronę przed atakami typu „phishing".
6. Rozwiązanie musi skanować wszystkie typów plików, zarówno w pamięci wewnętrznej, jak i na karcie SD, bez względu na ich rozszerzenie.
7. Rozwiązanie musi zapewniać co najmniej 2 poziomy skanowania: inteligentne i dokładne.
8. Rozwiązanie musi posiadać ochronę proaktywną wykrywającą nieznane zagrożenia.
9. W przypadku wykrycia zagrożenia użytkownik musi otrzymać odpowiednie powiadomienie.
10. Rozwiązanie musi umożliwiać zdefiniowanie harmonogramu dla pełnego skanowania urządzenia.
11. Rozwiązanie musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności (w pełni naładowane i podłączone do ładowarki).

Skanowanie na żądanie:

12. Rozwiązanie musi mieć możliwość skanowania zainstalowanych aplikacji.
13. Informacje o skanowaniu mają być przechowywane w plikach dziennika.
14. Użytkownik ma mieć możliwość wyboru akcji jaka ma być podjęta w przypadku wykrycia zagrożenia, co najmniej: poddania kwarantannie, usunięcia oraz zignorowania.
15. Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia.

Polityka ustawień:

16. Administrator musi mieć wgląd w podstawowe ustawienia urządzenia, w tym co najmniej:

a. połączenie Wi-Fi,
b. GPS,
c. usługi lokalizacyjne,
d. pamięć,
e. roaming danych,
f. roaming połączeń,
g. nieznane źródła,
h. tryb debugowania,
i. komunikacja NFC,
j. szyfrowanie pamięci masowej,
k. urządzenie zrootowane.

Kontrola aplikacji:

17. Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji.
18. Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji.

Blokowanie aplikacji musi być możliwe w oparciu o:

a. nazwę aplikacji,
b. nazwę pakietu,
c. kategorię sklepu Google Play,
d. uprawnienia aplikacji,
e. pochodzenie aplikacji z nieznanego źródła

Zabezpieczenia urządzenia:

19. W ramach zabezpieczeń administrator musi mieć możliwość uruchomienia polityki zabezpieczeń, w której może określić co najmniej:
    a. minimalny poziom zabezpieczeń i złożoność blokady ekranu,
    b. maksymalną dopuszczaną liczbę błędnych prób odblokowania,
    c. odstęp czasu, po którym użytkownik musi zmienić kod odblokowujący urządzenie,
    d. czas, po którym automatycznie nastąpi blokada ekranu,
    e. ograniczenie dostępu do kamery wbudowanej w urządzenie.

Aktualizacje modułów:

20. Rozwiązanie musi umożliwiać wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji.
21. Rozwiązanie musi mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje modułów co najmniej: raz dziennie, co 3 dni, co tydzień, co 6 godzin.
22. Rozwiązanie musi posiadać możliwość zabezpieczenia hasłem konkretnych modułów, w tym co najmniej: dostępu do ustawień ochrony antywirusowej, ochrony przed kradzieżą, deinstalacją.

Konfiguracja i zdalne zarządzanie:

23. Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne.
24. Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją.

Ochrona serwera Windows

1. Rozwiązanie musi posiadać wsparcie dla systemów Microsoft Windows Server 2012 i nowszych.
2. Instalator rozwiązania musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.
3. Rozwiązanie musi zapewniać pełną ochronę przed wirusami, trojanami, robakami i innymi zagrożeniami.
4. Rozwiązanie musi zapewniać wykrywanie i usuwanie niebezpiecznych aplikacji typu adware, spyware, dialer, phishing, narzędzi hakerskich, backdoor.
5. Rozwiązanie musi posiadać wbudowaną technologię do ochrony przed rootkitami.
6. Rozwiązanie musi wykrywać potencjalnie niepożądane, niebezpieczne oraz podejrzane aplikacje.
7. Rozwiązanie musi posiadać możliwość skanowania w czasie rzeczywistym otwieranych, tworzonych i wykonywanych plików.
8. Rozwiązanie musi posiadać możliwość skanowania całego dysku, wybranych katalogów, pojedynczych plików „na żądanie" lub według harmonogramu.
9. Rozwiązanie musi posiadać możliwość utworzenia wielu różnych zadań skanowania według harmonogramu. Każde zadanie może być uruchomione z innymi ustawieniami (metody skanowania, obiekty skanowania, czynności, rozszerzenia przeznaczone do skanowania,
   priorytet skanowania).
10. Rozwiązanie musi posiadać opcję skanowania „na żądanie" pojedynczych plików lub katalogów przy pomocy skrótu w menu kontekstowym.
11. Rozwiązanie musi posiadać możliwość określania priorytetu wykorzystania procesora (CPU) podczas skanowania „na żądanie" i według harmonogramu.
12. Rozwiązanie ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.
13. Rozwiązanie musi posiadać możliwość skanowania dysków sieciowych i dysków przenośnych.
14. Rozwiązanie musi posiadać możliwość skanowania plików spakowanych i skompresowanych.
15. Rozwiązanie musi posiadać możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
16. Rozwiązanie musi wspierać mechanizm klastrowania.
17. Rozwiązanie musi być wyposażone w system zapobiegania włamaniom działający na hoście (HIPS).
18. Moduł HIPS musi posiadać możliwość pracy w jednym z pięciu trybów:
    a. tryb automatyczny z regułami, gdzie program automatycznie tworzy i wykorzystuje reguły wraz z możliwością wykorzystania reguł utworzonych przez użytkownika,
    b. tryb interaktywny, w którym to rozwiązanie pyta użytkownika o akcję w przypadku wykrycia aktywności w systemie,
    c. tryb oparty na regułach, gdzie zastosowanie mają jedynie reguły utworzone przez użytkownika,
    d. 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,
    e. tryb inteligentny, w którym rozwiązanie będzie powiadamiało wyłącznie o

szczególnie podejrzanych zdarzeniach.

19. Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe, elementy docelowe rejestru systemowego.
20. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: pytaj, blokuj, zezwól.
21. Rozwiązanie musi posiadać zaawansowany skaner pamięci.
22. Rozwiązanie musi być wyposażone w mechanizm ochrony przed exploitami w popularnych aplikacjach, przynajmniej czytnikach PDF, aplikacjach JAVA, przeglądarkach internetowych.
23. Rozwiązanie musi oferować możliwość skanowania dysków sieciowych typu NAS.
24. Rozwiązanie musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na serwerze.
25. Rozwiązanie musi umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: Pamięci masowych, optycznych pamięci masowych, pamięci masowych Firewire, urządzeń do tworzenia obrazów, drukarek USB, urządzeń Bluetooth,
czytników kart inteligentnych, modemów, portów LPT/COM oraz urządzeń przenośnych.
26. Funkcja blokowania nośników wymiennych, bądź grup urządzeń ma umożliwiać użytkownikowi tworzenie reguł dla podłączanych urządzeń minimum w oparciu o typ, numer seryjny, dostawcę lub model urządzenia.
27. Rozwiązanie musi mieć możliwość utworzenia reguły na podstawie podłączonego urządzenia. Dana funkcjonalność musi pozwalać na automatyczne wypełnienie typu, numeru seryjnego, dostawcy oraz modelu urządzenia.
28. Rozwiązanie musi umożliwiać użytkownikowi nadanie uprawnień dla podłączanych urządzeń, w tym co najmniej: dostęp w trybie do odczytu, pełen dostęp, ostrzeżenie, brak dostępu do podłączanego urządzenia.
29. Rozwiązanie musi posiadać funkcjonalność, umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zalogowanego użytkownika.
30. Rozwiązanie musi posiadać funkcjonalność umożliwiającą zastosowanie reguł dla podłączanych urządzeń w zależności od zdefiniowanego przedziału czasowego.
31. W momencie podłączenia zewnętrznego nośnika aplikacja musi wyświetlić użytkownikowi odpowiedni komunikat i umożliwić natychmiastowe przeskanowanie całej zawartości podłączanego nośnika.
32. Rozwiązanie musi automatyczne wykrywać usługi zainstalowane na serwerze i tworzyć dla nich odpowiednie wyjątki.
33. Zainstalowanie na serwerze nowych usług serwerowych ma skutkować automatycznym dodaniem kolejnych wyłączeń w systemie ochrony.
34. Dodanie automatycznych wyłączeń nie wymaga restartu serwera.
35. Automatyczne wyłączenia mają być aktywne od momentu wykrycia usług serwerowych.
36. Administrator ma mieć możliwość wglądu w elementy dodane do wyłączeń i ich edycji.
37. Rozwiązanie nie może wymagać ponownego uruchomienia (restartu) komputera po instalacji.
38. Rozwiązanie ma mieć możliwość zmiany konfiguracji oraz wymuszania zadań z poziomu dedykowanego modułu CLI (command line).
39. Rozwiązanie musi posiadać możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.

40. Rozwiązanie musi posiadać dwa wbudowane niezależne moduły heurystyczne –jeden wykorzystujący pasywne metody heurystyczne i drugi wykorzystujący aktywne metodyheurystyczne oraz elementy sztucznej inteligencji. Musi istnieć możliwość wyboru z jaką heurystyką ma odbywać się skanowanie – z użyciem jednej lub obu metod jednocześnie.
41. Rozwiązanie musi posiadać możliwość automatycznego wysyłania nowych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika). Użytkownik musi mieć możliwość określenia rozszerzeń dla plików, które nie będą wysyłane automatycznie.
42. Rozwiązanie musi posiadać możliwość wysyłania wraz z próbką komentarza dotyczącego nowego zagrożenia i adresu e-mail użytkownika, na który producent może wysłać dodatkowe pytania dotyczące zgłaszanego zagrożenia.
43. Dane statystyczne zbierane przez producenta na podstawie otrzymanych próbek nowych zagrożeń mają być w pełni anonimowe.
44. Możliwość ręcznego wysłania próbki nowego zagrożenia z katalogu kwarantanny do laboratorium producenta.
45. W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.
46. Rozwiązanie musi posiadać możliwość zabezpieczenia konfiguracji hasłem, aby każdy użytkownik przy próbie dostępu do konfiguracji, był proszony o jego podanie.
47. Rozwiązanie musi posiadać możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.
48. Hasło do zabezpieczenia konfiguracji rozwiązania oraz deinstalacji musi być takie samo.
49. Rozwiązanie musi mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i wyświetlić listę niezainstalowanych aktualizacji.
50. Rozwiązanie musi mieć możliwość definiowania typu aktualizacji systemowych o braku, których będzie informował użytkownika w tym przynajmniej: aktualizacje krytyczne, aktualizacje ważne, aktualizacje zalecane oraz aktualizacje o niskim priorytecie. Ma być możliwość dezaktywacji tego mechanizmu.
51. Po instalacji rozwiązania, użytkownik ma mieć możliwość przygotowania płyty CD, DVD lub pamięci USB, z której będzie w stanie uruchomić komputer w przypadku infekcji i przeskanować dysk w poszukiwaniu zagrożeń.
52. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma umożliwiać pełną aktualizację silnika detekcji z Internetu lub z bazy zapisanej na dysku.
53. System antywirusowy, uruchomiony z płyty bootowalnej lub pamięci USB, ma pracować w trybie graficznym.
54. Rozwiązanie musi być wyposażone we wbudowaną funkcję, która wygeneruje pełny raport na temat stacji, na której został zainstalowany, w tym przynajmniej z: zainstalowanych aplikacji, usług systemowych, informacji o systemie operacyjnym i sprzęcie, aktywnych procesów i
połączeń sieciowych, harmonogramu systemu operacyjnego, pliku hosts, sterowników.
55. 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.
56. Rozwiązanie musi oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.

57. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
58. Rozwiązanie musi posiadać możliwość utworzenia kilku zadań aktualizacji. Każde zadanie musi być uruchamiane przynajmniej z jedną z opcji: co godzinę, po zalogowaniu, po uruchomieniu komputera.
59. Rozwiązanie musi posiadać możliwość określenia maksymalnego wieku dla silnika detekcji, po upływie którego program zgłosi posiadanie nieaktualnego silnika detekcji.
60. Rozwiązanie musi posiadać funkcjonalność tworzenia lokalnego repozytorium aktualizacji modułów.
61. Rozwiązanie musi posiadać funkcjonalność udostępniania tworzonego repozytorium aktualizacji modułów za pomocą wbudowanego w program serwera HTTP.
62. Rozwiązanie musi być wyposażone w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji modułów w celu ich późniejszego przywrócenia (rollback).
63. Rozwiązanie musi być wyposażone tylko w jeden proces uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, antyspyware, metody heurystyczne).
64. Rozwiązanie musi wspierać skanowanie magazynu Hyper-V.
65. Rozwiązanie musi posiadać możliwość wykluczania ze skanowania procesów.
66. Rozwiązanie musi posiadać dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, dokonanych aktualizacji modułów i samego oprogramowania.
67. Rozwiązanie musi oferować możliwość przeskanowania pojedynczego pliku poprzez opcję „przeciągnij i upuść”.
68. Rozwiązanie musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.
69. Wbudowany skaner UEFI nie może posiadać dodatkowego interfejsu graficznego i musi być transparentny dla użytkownika aż do momentu wykrycia zagrożenia.
70. Rozwiązanie musi posiadać wbudowany system IDS z detekcją prób ataków, anomalii w pracy sieci oraz wykrywaniem aktywności wirusów sieciowych.
71. Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.
72. Rozwiązanie musi posiadać ochronę przed przyłączeniem komputera do sieci botnet.
73. Rozwiązanie musi mieć możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
74. Rozwiązanie musi oferować mechanizm przesyłania zainfekowanych plików do laboratorium producenta, celem ich analizy, przy czym administrator musi mieć możliwość określenia, czy wysyłane mają być wszystkie zainfekowane próbki lub wszystkie z wyłączeniem dokumentów.
75. Administrator musi posiadać możliwość określenia typu podejrzanych plików, jakie będą przesyłane do producenta, w tym co najmniej pliki wykonywalne, archiwa, skrypty, dokumenty.
76. Administrator musi posiadać możliwość wyłączenia z przesyłania do analizy producenta określonych plików i folderów.
77. Rozwiązanie musi posiadać możliwość skanowania plików i folderów, znajdujących się w usłudze chmurowej OneDrive.
78. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu

Ochrona serwera – Linux

Architektura rozwiązania

1. Rozwiązanie musi posiadać skaner antywirusowy i antyspyware.
2. Rozwiązanie musi umożliwiać skanowanie plików, plików spakowanych i archiwów samorozpakowujących.
3. Rozwiązanie musi działać w architekturze bazującej na technologii mikro-serwisów. Funkcjonalność ta musi zapewniać podwyższony poziom stabilności, w przypadku awarii jednego z komponentów rozwiązania, nie spowoduje to przerwania pracy całego procesu, a jedynie wymusi restart zawieszonego mikro-serwisu.
4. Rozwiązanie musi posiadać wbudowany mechanizm typu „watchdog". Monitoruje on tzw. stan zdrowia poszczególnych mikro-serwisów i automatycznie przeładowuje je w przypadku wykrycia zakłóceń w pracy mikro-serwisu.
5. Architektura rozwiązania musi pozwalać na uruchamianie poszczególnych mikroserwisów, tylko na czas realizacji funkcjonalności przez nie realizowanych, co pozwala w znaczącym stopniu ograniczyć wykorzystanie zasobów systemu operacyjnego.
6. Rozwiązanie musi wspierać wieloprocesorową i wielordzeniową architekturę, w celu zapewnienia maksymalnego zwiększenia wydajności.
7. Rozwiązanie musi posiadać wsparcie dla SecureBoot-a.
8. Rozwiązanie musi być wyposażone w moduł ochrony systemu plików w czasie rzeczywistym. Moduł nie może wymagać instalowania jakichkolwiek dodatkowych komponentów w systemie operacyjnym. Wszystkie komponenty muszą być instalowane w systemie, podczas instalacji z dostarczonego instalatora binarnego.
9. Silnik ochrony systemu plików w czasie rzeczywistym musi stanowić dodatkowy moduł jądra systemu Linux i musi być dodawany do jądra, podczas procesu instalacji oprogramowania antywirusowego.
10. Ochrona systemu plików w czasie rzeczywistym musi być zapewniona nieprzerwanie od uruchomienia produktu i obejmuje skanowanie zarówno dysków lokalnych jak i zmapowanych dysków sieciowych.
11. Silnik skanujący musi działać wyłącznie z wykorzystaniem 64-bitowej architektury.
12. Rozwiązanie musi być w pełni zgodne z modułem SELinux, pracującym zarówno w trybie „Permissive" jak i „Enforcing".
13. Rozwiązanie podczas procesu instalacji, musi dodawać i konfigurować własne polityki modułu SELinux, które są kompatybilne z następującymi dystrybucjami systemów Linux: RedHat Enterprise Linux 7, Red Hat Enterprise Linux 8, Centos 7.
14. Wszystkie mechanizmy bezpieczeństwa rozwiązania muszą wspierać system informowania o zagrożeniach w czasie rzeczywistym. System ten pozwala na weryfikowanie reputacji plików oraz procesów i identyfikację nowych i nieznanych zagrożeń.
15. Skaner systemu plików w czasie rzeczywistym musi działać dla operacji obsługi plików, dla co najmniej takich operacji jak: dostęp do pliku, utworzenie (zapisanie) pliku.
16. Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach.
17. Administrator ma możliwość dodania wykluczenia dla zagrożenia po nazwie, sumie kontrolnej (SHA1) oraz lokalizacji pliku.
18. Rozwiązanie musi być wyposażone we własny wiersz polecenia (CLI). Polecenia muszą

być odpowiedzialne co najmniej za: skanowanie na żądanie, konfigurację mechanizmów bezpieczeństwa, uruchamianie aktualizacji, przeglądanie logów aplikacji, konfigurację graficznego interfejsu użytkownika, obsługę kwarantanny plików.

19. Rozwiązanie musi wspierać system plików zamontowany z flagą „noexec".
20. Rozwiązanie musi pozwalać na uruchamianie zadań skanowania działających ,,w tle",z możliwością ustawienia dla nich niskiego priorytetu.
21. Zadania skanowania nie mogą zmieniać znacznika dostępu do plików

Interfejs graficzny

1. Rozwiązanie musi pozwalać, na uruchomienie lokalnej konsoli administracyjnej, działającej z poziomu przeglądarki internetowej.
2. Lokalna konsola administracyjna musi działać w oparciu o dynamicznie generowaną zawartość tworzoną z wykorzystaniem następujących technologii: React/Node.js, HTML5.
3. Lokalna konsola administracyjna nie może wymagać do swojej pracy, uruchomienia i instalacji dodatkowego rozwiązania w postaci usługi serwera Web.
4. Lokalna konsola administracyjna musi zapewniać bezpieczne połączenie działające w oparciu o protokół HTTPS.
5. Lokalna konsola administracyjna musi umożliwiać uruchomienie jej, na wskazanym porcie TCP.
6. Logowanie do lokalnej konsoli administracyjnej musi być realizowane, poprzez podanie danych w postaci nazwy użytkownika i zdefiniowanego dla niego hasła.
7. Lokalna konsola administracyjna musi zapewniać funkcjonalność zweryfikowania stanu licencji i informacji na jej temat.
8. Z poziomu lokalnej konsoli administracyjnej musi być możliwość zarządzania, wbudowanym modułem menadżera kwarantanny.
9. Lokalna konsola administracyjna musi zapewniać możliwość przełączenia wersji językowej konsoli, na etapie logowania. Lokalna konsola administracyjna musi posiadać interfejs, co najmniej języku: polskim, angielskim, niemieckim, francuskim, hiszpańskim, japońskim.

Skanowanie sieciowych systemów plików

1. Rozwiązanie musi pozwalać na skanowanie plików składowanych i obsługiwanych przez zewnętrzne rozwiązania obsługi danych typu NAS / SAN.
2. Rozwiązanie nie może wymagać instalacji jakichkolwiek dodatkowych modułów na rozwiązaniach typu NAS / SAN, a skanowanie plików musi się odbywać wyłącznie w oparciu o protokół ICAP.
3. Rozwiązanie musi umożliwiać zmianę domyślnego portu protokołu ICAP.
4. Rozwiązanie, do celów skanowania plików na macierzach NAS / SAN, musi w pełni wspierać rozwiązanie Dell EMC Isilon.

Instalacja

1. Rozwiązanie musi wspierać mechanizm instalacji zdalnej, realizowanej przez narzędzia do orkiestracji systemami operacyjnymi. Wspieranymi narzędziami muszą być co najmniej: Puppet, Chef, Ansible.
2. Rozwiązanie musi być wyposażone w mechanizm automatycznej aktualizacji

komponentów programu.

3. Rozwiązanie musi posiadać automatyczną, inkrementacyjną aktualizację silnika detekcji.
4. Rozwiązanie musi wspierać następujące systemy operacyjne: RedHat Enterprise Linux (RHEL), CentOS, Ubuntu Server, Debian, SUSE Linux Enterprise Server (SLES), Oracle Linux, Amazon Linux oraz Alma Linux.

Licencjonowanie

1. Wsparcie techniczne do programu świadczone w języku polskim przez polskiego dystrybutora autoryzowanego przez producenta programu.
2. Rozwiązanie musi posiadać możliwość aktywacji przy użyciu co najmniej jednej z trzech metod: poprzez podanie poświadczeń administratora licencji, klucza licencyjnego lub aktywacji rozwiązania w trybie offline.

Administracja zdalna

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012, 2016, 2019, 2022 oraz systemach Linux.
2. Serwer zarządzający musi być dostępny w postaci gotowej maszyny wirtualnej w formacie OVA (Open Virtual Appliance) oraz dysku wirtualnego w formacie VHD.
3. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
4. Konsola administracyjna musi umożliwiać podgląd szczegółów, dotyczących bazy danych takich jak: serwer, nazwa, aktualny rozmiar, nazwa hosta, użytkownik.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość pobrania wszystkich wymaganych elementów serwera centralnej administracji w postaci jednego pakietu instalacyjnego i każdego z modułów oddzielnie bezpośrednio ze strony producenta.
7. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
8. Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy.
9. Narzędzie administracyjne musi być kompatybilne z protokołami IPv4 oraz IPv6.
10. Podczas logowania do konsoli, administrator musi mieć możliwość wyboru języka, w jakim zostanie wyświetlony interfejs.
11. Zmiana języka interfejsu konsoli nie może wymagać jej zatrzymania, ani reinstalacji.
12. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
13. Konsola administracyjna musi ostrzegać administratora, kiedy używa niewspieranej przeglądarki, do administracji rozwiązaniem antywirusowym.
14. Narzędzie do administracji zdalnej musi posiadać moduł, pozwalający na wykrycie niezarządzanych stacji roboczych w sieci.
15. Serwer administracyjny musi posiadać mechanizm instalacji zdalnej agenta na stacjach roboczych.
16. Serwer administracyjny musi posiadać mechanizm wykrywający sklonowane maszyny na podstawie unikatowego identyfikatora sprzętowego stacji.
17. Serwer administracyjny musi posiadać wsparcie dla „VDI" oraz „Golden Master Image".
18. Serwer administracyjny musi posiadać możliwość podłączenia 250 000 hostów.
19. Instalacja serwera administracyjnego powinna posiadać możliwość pracy w sieci rozproszonej, nie wymagając dodatkowego serwera proxy.
20. Rozwiązanie ma posiadać możliwość komunikacji agenta przy wykorzystaniu HTTP Proxy.

21. Administrator musi posiadać możliwość instalacji serwera HTTP Proxy, pozwalającego na pobieranie aktualizacji silnika detekcji oraz pakietów instalacyjnych na stacjach roboczych.
22. Serwer HTTP Proxy musi posiadać mechanizm zapisywania w pamięci podręcznej (cache) pobieranych elementów.
23. Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.
24. Serwer administracyjny musi posiadać możliwość utworzenia własnego CA (Certification Authority) oraz dowolnej liczby certyfikatów z podziałem na typ elementu: agent, serwer zarządzający.
25. Serwer administracyjny musi pozwalać na zarządzanie programami zabezpieczającymi na maszynach z systemami Windows, MacOS, Linux.
26. Serwer administracyjny musi pozwalać na centralną konfigurację i zarządzanie przynajmniej takimi modułami jak: ochrona antywirusowa, zapora osobista, kontrola dostępu do stron internetowych, które działają na stacjach roboczych w sieci.
27. Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.
28. Administrator musi posiadać możliwość zarządzania stacjami roboczymi za pomocą dedykowanego agenta, na których nie jest zainstalowane oprogramowanie zabezpieczające.
29. Z poziomu konsoli zarządzania administrator ma mieć możliwość weryfikacji podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, typ i wersja oprogramowania układowego, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich dla systemów Windows oraz MacOS z możliwością jego odinstalowania.
30. Serwer administracyjny musi posiadać możliwość wymuszenia połączenia agenta do serwera administracyjnego z pominięciem domyślnego czasu oczekiwania na połączenie.
31. Instalacja zdalna agenta z poziomu serwera administracyjnego nie może wymagać określenia architektury systemu (32 lub 64 bitowy) oraz jego rodzaju (Windows, MacOS, Linux), a wybór odpowiedniego pakietu musi być w pełni automatyczny.
32. Administrator musi posiadać możliwość utworzenia użytkownika serwera administracyjnego.
33. Administrator musi posiadać możliwość dodania grupy użytkowników z Active Directory do serwera administracyjnego. Użytkownik grupy usługi katalogowej Active Directory musi mieć możliwość logowania się do konsoli administracyjnej swoimi poświadczeniami domenowymi. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
34. Serwer administracyjny musi posiadać możliwość dodania zestawu uprawnień dla użytkowników w oparciu co najmniej o funkcje zarządzania: politykami, instalacją agentów, raportowaniem, zarządzaniem licencjami, zadaniami administracyjnymi. Każda z funkcji musi posiadać możliwość wyboru uprawnienia: odczyt, użyj, zapisz oraz brak.
35. Administrator musi posiadać możliwość przypisania kilku zestawów uprawnień do jednego użytkownika.
36. Użytkownik musi posiadać możliwość zmiany hasła dla swojego konta, bez konieczności logowania się do konsoli administracyjnej.
37. Serwer administracyjny musi posiadać możliwość konfiguracji czasu bezczynności, po którym użytkownik zostanie automatycznie wylogowany.
38. Serwer administracyjny musi posiadać zadania klienta oraz zadania serwera. Zadania

serwera muszą zawierać przynajmniej zadanie instalacji agenta, generowania raportów oraz synchronizacji elementów z Active Directory. Zadania klienta muszą być wykonywane za pośrednictwem agenta na stacji roboczej.

39. Agent musi posiadać mechanizm pozwalający na zapis zadania w swojej pamięci wewnętrznej w celu ich późniejszego wykonania bez względu na stan połączenia z serwerem centralnej administracji.
40. Serwer administracyjny musi posiadać możliwość instalacji oprogramowania z użyciem parametrów instalacyjnych.
41. Serwer administracyjny musi posiadać możliwość deinstalacji programu zabezpieczającego firm trzecich, zgodnych z technologią OPSWAT.
42. Serwer administracyjny musi posiadać możliwość wysłania polecenia: wyświetlenia komunikatu, aktualizacji systemu operacyjnego, zamknięcia komputera, uruchomienia ponownego komputera oraz uruchomienia komendy na stacji klienckiej.
43. Serwer administracyjny musi posiadać możliwość uruchomienia zadania automatycznie, przynajmniej z wyzwalaczem: wyrażenie CRON, codziennie, cotygodniowo, comiesięcznie, corocznie, po wystąpieniu nowego zdarzenia oraz umieszczeniu agenta w grupie dynamicznej.
44. Serwer administracyjny musi posiadać możliwość tworzenia grup statycznych i dynamicznych komputerów.
45. Grupy dynamiczne muszą być tworzone na podstawie szablonu określającego warunki, jakie musi spełnić klient, aby został umieszczony w danej grupie. Warunki muszą zawierać co najmniej: adresy sieciowe IP, aktywne zagrożenia, stan funkcjonowania/ochrony, wersja systemu operacyjnego, podzespoły komputera.
46. Serwer administracyjny musi posiadać możliwość utworzenia polityk dla programów zabezpieczających i komponentów środowiska serwera centralnego zarządzania.
47. Serwer administracyjny musi posiadać możliwość przypisania polityki dla pojedynczego klienta lub dla grupy komputerów.
48. Serwer administracyjny musi posiadać możliwość przypisania kilku polityk z innymi priorytetami dla pojedynczego klienta.
49. Edytor konfiguracji polityki musi być identyczny jak edytor konfiguracji ustawień w programie zabezpieczającym na stacji roboczej.
50. Serwer administracyjny musi umożliwiać wyświetlenie polityk, które są przypisane do stacji.
51. Z poziomu konsoli musi istnieć możliwość scalania reguł zapory osobistej, harmonogramu, modułu HIPS z już istniejącymi regułami na stacji roboczej lub innej polityce.
52. Serwer administracyjny musi posiadać minimum 120 szablonów raportów, przygotowanych przez producenta.
53. Serwer administracyjny musi posiadać możliwość utworzenia własnych raportów.
54. Serwer administracyjny musi posiadać możliwość wyboru formy przedstawienia danych w raporcie w tym przynajmniej: w postaci tabeli, wykresu lub obu elementów jednocześnie.
55. Serwer administracyjny musi posiadać możliwość wyboru jednego z kilku typów wykresów: kołowy, pierścieniowy, liniowy, słupkowy, punktowy.
56. Serwer administracyjny musi posiadać możliwość określenia danych, jakie powinny znajdować się w poszczególnych kolumnach tabeli lub na osiach wykresu oraz ich odfiltrowania i posortowania.
57. Serwer administracyjny musi być wyposażony w mechanizm importu oraz

eksportu szablonów raportów.

58. Serwer administracyjny powinien posiadać panel kontrolny z raportami, pozwalający na szybki dostępu do najbardziej interesujących danych. Panel ten musi być edytowalny.
59. Serwer administracyjny musi posiadać możliwość wygenerowania raportu na żądanie, zgodnie z harmonogramem lub umieszczenia raportu na panelu kontrolnym. Raport może zostać wysłany za pośrednictwem wiadomości email, zapisany do pliku w formacie PDF lub CSV.
60. Raport na panelu kontrolnym musi być w pełni interaktywny, pozwalając przejść do zarządzania stacją/stacjami, której raport dotyczy.
61. Serwer administracyjny musi posiadać możliwość utworzenia własnych powiadomień lub skorzystania z predefiniowanych wzorów.
62. Powiadomienia mailowe mają być wysyłane w formacie HTML.
63. Powiadomienia muszą być wywoływane po zmianie ilości członków danej grupy dynamicznej, wzroście liczby klientów grupy w stosunku do innej grupy, pojawienia się dziennika zagrożeń.Administrator musi posiadać możliwość wysłania powiadomienia przynajmniej za pośrednictwem wiadomości email, komunikatu SNMP oraz do dziennika syslog.
64. Serwer administracyjny musi posiadać możliwość agregacji identycznych powiadomień występujących w zadanym przez administratora okresie czasu.
65. Serwer administracyjny musi posiadać możliwość synchronizacji danych dotyczących licencji.
66. Serwer administracyjny musi posiadać możliwość dodania licencji przynajmniej przy użyciu klucza licencyjnego, pliku offline licencji oraz konta systemu zarządzania licencjami.
67. Serwer administracyjny musi posiadać możliwość dodania dowolnej ilości licencji produktów zarządzanych.
68. W przypadku posiadania tylko jednej dodanej licencji w konsoli zarządzania ma być ona wybierana automatycznie podczas konfiguracji zadania aktywacji lub instalacji produktu.
69. Serwer administracyjny musi posiadać możliwość weryfikacji identyfikatora publicznego licencji, ilości wykorzystanych stanowisk, czasu wygaśnięcia, wersji produktu, na który jest licencja oraz jej właściciela.
70. Serwer administracyjny musi posiadać możliwość wybudzania stacji roboczych przy użyciu Wake on Lan.
71. Serwer musi umożliwić podział uprawnień administratorów w taki sposób, aby każdy z nich miał możliwość zarządzania konkretnymi grupami komputerów, politykami oraz zadaniami.
72. Serwer ma posiadać możliwość wygenerowania dziennika diagnostycznego na stacji roboczej, który może zostać pobrany bezpośrednio z konsoli.
73. W szczegółach stacji roboczej, z poziomu konsoli, muszą być dostępne zaawansowane logi diagnostyczne, przynajmniej z modułów produktu zabezpieczającego, takich jak: HIPS, kontrola dostępu do urządzeń.
74. Konsola webowa musi zawierać informacje, dotyczące wysłanych plików do analizy producenta.
75. Administrator musi mieć możliwość pobrania pliku z parametrami połączenia RDP do stacji roboczej bezpośrednio z poziomu konsoli.
76. Na panelu kontrolnym musi być dostępny dziennik zmian, dotyczący produktów zabezpieczających i komponentów środowiska centralnego zarządzania.

77. Serwer musi wspierać wysyłanie logów do systemu SIEM IBM qRadar w jego natywnym formacie.
78. Konsola administracyjna musi umożliwiać personalizację interfejsu webowego.
79. Konsola administracyjna musi mieć możliwość tagowania obiektów, w tym przynajmniej: polityki, zadania, komputery oraz szablony grupy dynamicznych.
80. Konsola administracyjna musi mieć możliwość zarządzania rozwiązaniem do szyfrowania całej powierzchni dysku, które pochodzi od tego samego producenta oraz posiadać możliwość zarządzania natywnym szyfrowaniem dla systemów macOS (FileVault).
81. Konsola administracyjna musi pozwalać na utworzenie wykluczeń globalnych, bez konieczności przypisywania ich do konkretnych polityk.
82. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, wykrytego przez produkt antywirusowy, na portalach służących do weryfikacji bezpieczeństwa (co najmniej VirusTotal).
83. Konsola administracyjna musi posiadać możliwość wyświetlania dziennika audytu czynności wykonanych przez administratorów serwera. Dziennik musi pozwalać na wyświetlanie informacji co najmniej ze zmian dotyczących: certyfikatów, zadań, wyzwalaczy, konfiguracji, grup, uprawnień administratorów, wykluczeń, powiadomień, raportów.

Szyfrowanie

1. System szyfrowania danych musi wspierać instalację aplikacji klienckiej w środowisku Microsoft Windows 10 i Microsoft Windows 11.
2. System szyfrowania musi wspierać zarządzanie natywnym szyfrowaniem w systemach macOS (FileVault).
3. Aplikacja musi posiadać autentykacje typu Pre-boot, czyli uwierzytelnienie użytkownika zanim zostanie uruchomiony system operacyjny. Musi istnieć także możliwość całkowitego lub czasowego wyłączenia tego uwierzytelnienia.
4. Aplikacja musi być dostępna, przynajmniej w języku polskim i angielskim.
5. Szyfrowanie pełnej powierzchni dysku musi umożliwiać wykorzystanie modułu TPM.
6. Aplikacja musi mieć możliwość korzystania z technologii TCG OPAL - dyski sprzętowo szyfrowane.
7. Aplikacja musi umożliwiać szyfrowanie danych tylko na komputerach z UEFI.
8. W przypadku utraty hasła, aplikacja musi umożliwiać użytkownikowi odzyskanie dostępu do zaszyfrowanego dysku, poprzez użycie otrzymanego od administratora jednorazowego hasła, wygenerowanego z poziomu konsoli centralnego zarządzania.
9. Aplikacja do szyfrowania musi być zarządzana z poziomu konsoli webowej, wykorzystywanej do zarządzania produktem do ochrony antywirusowej.
10. Konsola centralnego zarządzania musi pozwalać na wygenerowanie, dla każdej zaszyfrowanej stacji, dysku ratunkowego.
11. Musi istnieć możliwość konfiguracji złożoności hasła dla użytkowników na stacjach roboczych, w oparciu o przynajmniej:
    a. ilość znaków,
    b. czy hasło ma zawierać wielkie litery,
    c. czy hasło ma zawierać małe litery,
    d. czy hasło ma zawierać cyfry,
    e. czy hasło ma zawierać znaki specjalne,
    f. okres ważności,
    g. ilość nieudanych logowań,

h. możliwość zmiany hasła.

12. Aplikacja musi posiadać możliwość ograniczenia wyświetlania interfejsu graficznego użytkownikom.
13. Administrator musi posiadać możliwość zablokowania dostępu do zaszyfrowanego dysku.

Extended detection & response (XDR)

1. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
2. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
3. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
4. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
5. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
6. Administrator musi posiadać możliwość weryfikacji uruchomionych skryptów na stacjach roboczych, wraz z informacją dotyczącą parametrów uruchomienia. Administrator musi posiadać możliwość oznaczenia skryptu jako bezpieczny lub niebezpieczny.
7. W ramach przeglądania wykonanego skryptu, administrator musi posiadać możliwość szczegółowego podglądu wykonanych przez skrypt czynności w formie tekstowej. W ramach przeglądania wykonanego skryptu lub pliku exe, administrator musi posiadać
8. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
9. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
10. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.
11. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
12. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
13. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
14. Serwer administracyjny musi posiadać możliwość instalacji na systemach Windows Server 2012 i nowszych.
15. Serwer administracyjny musi wspierać instalację z użyciem nowego lub istniejącego serwera bazy danych MS SQL i MySQL.
16. System musi współpracować z serwerem administracyjnym produktu antywirusowego, tego samego producenta.
17. Dostęp do konsoli centralnego zarządzania musi odbywać się z poziomu interfejsu WWW.
18. Serwer administracyjny musi posiadać możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.
19. Serwer administracyjny musi posiadać możliwość wysyłania zdarzeń do konsoli administracyjnej tego samego producenta.
20. Interfejs musi być zabezpieczony za pośrednictwem protokołu SSL.
21. Serwer administracyjny musi posiadać możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa.

22. Wykluczenia muszą dotyczyć procesu lub procesu „rodzica".
23. Utworzenie wykluczenia musi automatycznie rozwiązywać alarmy, które pasują do utworzonego wykluczenia.
24. Kryteria wykluczeń muszą być konfigurowane w oparciu o przynajmniej: nazwę procesu, ścieżkę procesu, wiersz polecenia, wydawcę, typ podpisu, SHA-1, nazwę komputera, grupę, użytkownika.
25. Serwer musi posiadać wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Administrator musi też posiadać możliwość utworzenia własnych reguł i edycji reguł dodanych przez producenta.
26. Serwer administracyjny musi posiadać możliwość uruchomienia reguł w oparciu o dane historyczne.
27. Serwer administracyjny musi oferować możliwość blokowania plików po sumach kontrolnych. W ramach blokady musi istnieć możliwość dodania komentarza oraz konfiguracji wykonywanej czynności, po wykryciu wprowadzonej sumy kontrolnej.
28. Serwer musi posiadać możliwość ustawiania priorytetu zdarzeń z użyciem 4-stopniowej skali.
29. Administrator musi posiadać możliwość weryfikacji uruchomionych plików wykonywalnych na stacji roboczej z możliwością podglądu szczegółów wybranego procesu przynajmniej o: SHA-1, typ podpisu, wydawcę, opis pliku, wersję pliku, nazwę firmy, nazwę produktu, wersję produktu, oryginalną nazwę pliku, rozmiar pliku oraz reputację i popularność pliku.
30. Administrator, w ramach plików wykonywalnych oraz plików DLL, musi posiadać możliwość ich oznaczenia jako bezpieczne, pobrania do analizy oraz ich zablokowania.
31. możliwość weryfikacji powiązanych zdarzeń dotyczących przynajmniej: modyfikacji plików i rejestru, zestawionych połączeń sieciowych i utworzonych plików wykonywalnych.
32. Serwer administracyjny musi posiadać funkcję wyszukiwarki, w której administrator jest w stanie wyszukać dowolny element lub zdarzenie na podstawie wprowadzonej nazwy.
33. Serwer administracyjny musi oferować możliwość przekierowania do konsoli zarządzającej produktu antywirusowego tego samego producenta, w celu weryfikacji szczegółów wybranej stacji roboczej. W konsoli zarządzającej produktu antywirusowego, administrator musi mieć możliwość podglądu informacji dotyczących przynajmniej: podzespołów zarządzanego komputera (w tym przynajmniej: producent, model, numer seryjny, informacje o systemie, procesor, pamięć RAM, wykorzystanie dysku twardego, informacje o wyświetlaczu, urządzenia peryferyjne, urządzenia audio, drukarki, karty sieciowe, urządzenia masowe) oraz wylistowanie zainstalowanego oprogramowania firm trzecich.
34. Serwer administracyjny musi oferować możliwość bezpośredniego sprawdzenia SHA-1 pliku, na portalach służących do weryfikacji bezpieczeństwa (np. VirusTotal).
35. Administrator musi posiadać możliwość wymuszenia dwufazowej autoryzacji podczas logowania do konsoli administracyjnej.
36. Konsola administracyjna musi mieć możliwość tagowania obiektów.
37. Konsola administracyjna musi umożliwiać audytowanie innych administratorów konsoli.
38. Konsola administracyjna musi pozwalać na włączenie izolacji komputera od sieci.
39. Konsola administracyjna musi umożliwiać połączenie się do stacji roboczej z możliwością wykonywania poleceń powershell.
40. Konsola administracyjna musi umożliwiać dodawanie emotikon do co najmniej komentarzy, tagów, nazw reguł.

Konektor

1. Pełne wsparcie dla systemu Windows 10/ Windows 11 oraz Windows Server 2012/2012R2/2016/2019/2022.
2. Pełne wsparcie dla systemów macOS 10.15 i nowszych.
3. Pełne wsparcie dla systemów Linux RHEL 7.6+/RHEL 8/RHEL 9/Ubuntu 18.04/Ubuntu 20.04/Ubuntu 22.04/Debian 10/Debian 11/Debian 12
4. Wsparcie dla 32 i 64-bitowej wersji systemu Windows.
5. Konektor musi współpracować z produktem antywirusowym tego samego producenta.
6. Konektor nie może działać bez produktu antywirusowego tego samego producenta.
7. W ramach wprowadzonych reguł administracyjnych dotyczących blokowania/usuwania plików, użytkownik musi otrzymać stosowne powiadomienie, dotyczące czynności wykonane przez konektor.
8. Połączenie konektora do serwera zarządzającego musi być szyfrowane.
9. Administrator musi posiadać możliwość utworzenia polityki z konsoli administracyjnej zawierającej wykluczenia dla procesów, które nie będą analizowane.

Sandbox w chmurze

1. Rozwiązanie musi zapewniać ochronę przed zagrożeniami 0-day.
2. Rozwiązanie musi wykorzystywać do działania chmurę producenta.
3. Rozwiązanie musi posiadać możliwość określenia jakie pliki mają zostać przesłane do chmury automatycznie, w tym archiwa, skrypty, pliki wykonywalne, możliwy spam, dokumenty oraz inne pliki typu .jar, .reg, .msi.
4. Administrator musi mieć możliwość zdefiniowania po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.
5. Administrator musi mieć możliwość zdefiniowania maksymalnego rozmiaru przesyłanych próbek.
6. Rozwiązanie musi pozwalać na utworzenie listy wykluczeń określonych plików lub folderów z przesyłania.
7. Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.
8. Administrator musi mieć możliwość podejrzenia listy plików, które zostały przesłane do analizy.
9. Rozwiązanie musi pozwalać na analizowanie plików, bez względu na lokalizacje stacji roboczej. W przypadku wykrycia zagrożenia, całe środowisko jest bezzwłocznie chronione.
10. Rozwiązanie nie może wymagać instalacji dodatkowego agenta na stacjach roboczych.
11. Rozwiązanie pozwala na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora, za pomocą wspieranego produktu. Administrator musi móc podejrzeć jakie pliki zostały wysłane do analizy oraz przez kogo.
12. Przeanalizowane pliki muszą zostać odpowiednio oznaczone. Analiza pliku może zakończyć się z wynikiem:
    a. Czysty,
    b. Podejrzany,
    c. Bardzo podejrzany,
    d. Szkodliwy.
13. W przypadku stacji roboczych rozwiązanie musi posiadać możliwość wstrzymania

uruchamiania pobieranych plików za pośrednictwem przeglądarek internetowych, klientów poczty e-mail, z nośników wymiennych oraz wyodrębnionych z archiwum.

14. W przypadku serwerów pocztowych rozwiązanie musi posiadać możliwość wstrzymania dostarczania wiadomości do momentu zakończenia analizy próbki.
15. Wykryte zagrożenia muszą być przeniesione w bezpieczny obszar kwarantanny, z której administrator może przywrócić dowolne pliki oraz utworzyć dla niej wyłączenia.