Numer JRWA: IT-02-2.1333.10.2024 ***Wzór umowy***

Numer Umowy:

UMOWA

zawarta w dniu określonym na podstawie § 8 ust. 11 pomiędzy:

Gminą Miejską Kraków z siedzibą w Krakowie, pl. Wszystkich Świętych 3-4, 31-004 Kraków, NIP: 676-101-37-17, REGON: 351554353, zwaną dalej **Zamawiającym**, reprezentowaną przez:

…… – ……,

……,

a

……

…… – ……,

zwani dalej z osobna **Stroną**, a łącznie **Stronami**.

Umowa niniejsza (dalej: Umowa) została zawarta w wyniku udzielenia zamówienia publicznego w trybie podstawowym zgodnie z art. 275 pkt 1 ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (t. j.: Dz. U. z 2024 r. poz. 1320) przez Urząd Miasta Krakowa tj. zamawiającego w rozumieniu art. 7 pkt 31 ww. ustawy.
Znak sprawy: IT-03-2.271.15.2024.
Umowę zawiera się na podstawie § 2 ust. 1 pkt 2 aktualnej Wieloletniej Prognozy Finansowej Miasta Krakowa - zapewnienie ciągłości działania systemu informatycznego UMK .

§ 1

Przedmiot umowy i termin realizacji

1. Przedmiotem Umowy jest:
   1) dostarczenie przez Wykonawcę na rzecz Zamawiającego oprogramowania XDR - …… (dalej: Oprogramowania) dla 1000 urządzeń w formie subskrypcji, szczegółowo opisanego w Załączniku nr 1 do Umowy,
   2) świadczenie przez Wykonawcę na rzecz Zamawiającego usługi wsparcia technicznego dla Oprogramowania, o którym mowa w pkt 1, w wymiarze 60 godzin, do wykorzystania przez okres ważności subskrypcji, o którym mowa w ust. 2.
2. Przedmiot Umowy, o których mowa w ust. 1 pkt 1 zostanie dostarczony do 14 dni od dnia zawarcia Umowy i będzie aktywny przez okres 36 miesięcy od dnia, o którym mowa w § 2 ust. 2.
3. Wsparcie techniczne, o którym mowa w ust. 1 pkt 2, obejmować będzie wykrywanie przez Wykonawcę zagrożeń cybernetycznych w oparciu o zaawansowane wyszukiwania zachowań niecharakterystycznych i złośliwych w środowisku produkcyjnym Zamawiającego i polegać będzie na konsultacjach telefonicznych z Wykonawcą pod numerem telefonu: …….. lub za pośrednictwem poczty elektronicznej pomiędzy osobami

odpowiedzialnymi za realizację Umowy, o których mowa w § 3 ust. 23-24.

§ 2

Odbiór przedmiotu Umowy

1. Dostarczenie przedmiotu Umowy, o którym mowa w § 1 ust. 1, tj. potwierdzenie nabycia subskrypcji wraz z dostępem do konsoli chmurowej usługi bezpieczeństwa, zostanie przekazane Zamawiającemu w formie wiadomości e-mail przesłanej na adres poczty elektronicznej: .....
2. Za dzień nabycia subskrypcji rozumie się dzień przesłania wiadomości e-mail na adres poczty elektronicznej wskazany w ust. 1, pod warunkiem, że Zamawiający przy użyciu konsoli, o której mowa w ust. 1, potwierdzi poprawność dostarczonych subskrypcji (za pośrednictwem wiadomości e-mail na adres, z którego została przesłana wiadomość, o której mowa w ust. 1).
3. Wykonawca oświadcza, że jest uprawniony do zawarcia Umowy i wykonania jej przedmiotu.

§ 3

Rozliczenie finansowe

1. Za wykonanie przedmiotu Umowy, o którym mowa w § 1 ust. 1, Wykonawca otrzyma łączne wynagrodzenie w kwocie **..... brutto** (słownie: .....złotych .../100), w tym stawka VAT ...%, w tym za wykonanie przedmiotu Umowy, o którym mowa w:
   1) § 1 ust. 1 pkt 1 – ..... złotych brutto (słownie: ..... złotych .../100),
   2) § 1 ust. 1 pkt 2 – ..... złotych brutto (słownie: ..... złotych .../100).
2. Wynagrodzenie, o którym mowa w ust. 1 pkt 1, zostanie wypłacone Wykonawcy przez Zamawiającego w trzech równych częściach w wysokości ..... złotych brutto (słownie:..... złotych .../100), za realizację przedmiotu Umowy, o którym mowa w § 1 ust. 1 pkt 1, z góry za każde pełne 12 miesięcy obowiązywania Umowy (dalej: Rok Rozliczeniowy), na podstawie prawidłowo sporządzonych i przedłożonych przez Wykonawcę faktur, w terminie do 30 dni od dnia ich otrzymania, jednak nie później niż do 20 grudnia danego roku.
3. Podstawą do wystawienia faktur, o których mowa w ust. 2:
   1) w pierwszym Roku Rozliczeniowym jest potwierdzenie Zamawiającego, o którym mowa w § 2 ust. 2. Faktura zostanie wystawiona przez Wykonawcę do 7 dni od dnia potwierdzenia przez Zamawiającego, a w przypadku faktury wystawianej w miesiącu grudniu – nie później niż do 16 grudnia danego roku.
   2) w drugim i trzecim Roku Rozliczeniowym jest upływ 12 i 24 miesięcy od dnia otrzymania potwierdzenia Zamawiającego, o którym mowa w § 2 ust. 2. Faktury zostaną wystawione przez Wykonawcę do 7 dni od ww. terminów, a w przypadku faktur wystawianych w miesiącu grudniu – nie później niż do 16 grudnia danego roku.
4. Wynagrodzenie, o którym mowa w ust. 1 pkt 2, będzie wypłacane Wykonawcy z dołu za każde pełne 3 miesiące obowiązywania Umowy (dalej: Kwartał Rozliczeniowy) na podstawie prawidłowo sporządzonych i przedłożonych przez Wykonawcę faktur, w terminie do 30 dni od dnia ich otrzymania (jednak nie później niż do

20 grudnia danego roku), za wykonane wsparcie techniczne w danym Kwartale Rozliczeniowym i stanowić będzie iloczyn godzin zrealizowanych przez Wykonawcę w ramach wsparcia technicznego oraz stawki godzinowej.

5. Stawka godzinowa, o której mowa w ust. 4 , wynosi … **złotych brutto** (słownie: … złotych …/100) i ma charakter ryczałtowy, obejmuje wszelkie koszty jakie Wykonawca poniesie w związku z realizacją wsparcia technicznego.
6. Czas udzielania wsparcia technicznego naliczany będzie w trzydziestominutowych segmentach, za każde rozpoczęte trzydzieści minut. Zamawiający i Wykonawca ustalają, iż koszt trzydziestominutowego segmentu będzie wynosić ½ stawki godzinowej, określonej w ust. 5
7. Podstawą do wystawienia faktur, o których mowa w ust. 4 jest zaakceptowany raport o wsparciu technicznym, o którym mowa w ust. 9. Faktury zostaną wystawione przez Wykonawcę do 7 dni od dnia akceptacji raportu przez Zamawiającego, a w przypadku faktury wystawianej w miesiącu grudniu – nie później niż do 16 grudnia danego roku.
8. Po zakończeniu każdego Kwartału Rozliczeniowego, o którym mowa w ust. 4, Wykonawca sporządza pisemny raport, wykazujący zrealizowane w danym Kwartale Rozliczeniowym wsparcie techniczne oraz liczbę godzin poświęconych na realizację wsparcia technicznego, z zastrzeżeniem, iż raport sporządza się wyłącznie w przypadku, gdy wsparcie techniczne było realizowane w danym Kwartale Rozliczeniowym Wzór raportu stanowi Załącznik nr 2 do Umowy. Wykonawca przesyła raport Zamawiającemu w terminie do 3 Dni roboczych od zakończenia Kwartału Rozliczeniowego.
9. Zamawiający weryfikuje treść raportu i akceptuje ilość godzin wsparcia technicznego określonych w raporcie lub zgłasza uwagi dotyczące treści raportu. Wzór adnotacji umieszczanej na raporcie określa Załącznik nr 2 do Umowy. Skan raportu opatrzonego adnotacją o akceptacji lub braku akceptacji Zamawiający przesyła Wykonawcy na adres e-mail: ……. w ciągu 2 Dni roboczych od dnia otrzymania raportu od Wykonawcy. W przypadku braku akceptacji raportu przez Zamawiającego, procedura wskazana w ust. 8-9 zostanie powtórzona.
10. Podstawą do zapłaty prawidłowo sporządzonych i przedstawionych przez Wykonawcę faktur, o których mowa w ust. 2 i 4, będzie załączenie odpowiedniej adnotacji do faktury przez osobę wskazaną w ust. 23 lub osobę zastępującą.
11. Za dzień zapłaty uznaje się dzień obciążenia rachunku bankowego Zamawiającego.
12. Fakturę należy wystawić na Gminę Miejską Kraków, Plac Wszystkich Świętych 3-4, 31-004 Kraków, jednostka odbierająca: Urząd Miasta Krakowa – Centrum Obsługi Informatycznej, ul. Basztowa 20, 31-156 Kraków i dostarczyć w terminie do 7 dni od dnia jej wystawienia na adres: Gmina Miejska Kraków, Plac Wszystkich Świętych 3-4, 31-004 Kraków lub na adres e-mail: …….. lub przesłać za pośrednictwem Platformy Elektronicznego Fakturowania (PEF).
13. Wykonawca może wystawić i wysłać do Zamawiającego ustrukturyzowaną fakturę elektroniczną za pośrednictwem PEF.
14. Zamawiający zobowiązany jest do odbierania od Wykonawcy ustrukturyzowanych faktur elektronicznych przesłanych za pośrednictwem PEF.

15. Do wysyłania ustrukturyzowanych faktur elektronicznych Wykonawca wykorzystuje własne konto na PEF.
16. Prawidłowo wystawiona ustrukturyzowana faktura elektroniczna powinna zawierać następujące dane Zamawiającego:

    NABYWCA:

    Nazwa kontrahenta: Gmina Miejska Kraków

    NIP: 6761013717

    Typ numeru PEPPOL: GLN

    Numer PEPPOL: 5907662634251

    Adres: Plac Wszystkich Świętych 3-4, 31-004 Kraków

    ODBIORCA:

    Urząd Miasta Krakowa – Centrum Obsługi Informatycznej

    Adres: ul. Basztowa 20, 31-156 Kraków.
17. Terminem otrzymania ustrukturyzowanej faktury elektronicznej jest data dostępności faktury na PEF dla Zamawiającego potwierdzona otrzymaną wiadomością e-mail.
18. Zamawiający wyraża zgodę na przekazywanie przez Wykonawcę dokumentów elektronicznych innych niż ustrukturyzowana faktura elektroniczna za pośrednictwem PEF, tj.: faktur korygujących.
19. Zapłata wynagrodzenia nastąpi przelewem na rachunek bankowy Wykonawcy nr: ……..
20. Wykonawcy nie przysługuje żadne inne roszczenie o dodatkowe wynagrodzenie nieprzewidziane w Umowie. Zamawiający nie będzie zwracał Wykonawcy wydatków ani zwalniał go z zobowiązań zaciągniętych w celu wykonania Umowy.
21. Zamawiający jest podatnikiem podatku VAT. NIP: 676-101-37-17, REGON: 351554353.
22. Wykonawca *jest/nie jest* podatnikiem podatku VAT - *zwolniony*. NIP: ……., REGON: ……. . *W przypadku gdy Wykonawca w trakcie trwania Umowy zmieni swój status na status podatnika VAT, kwota wynagrodzenia zawarta w Umowie będzie traktowana jako kwota brutto.*
23. Osobą odpowiedzialną ze strony Zamawiającego za realizację Umowy jest *Pan/Pani* …….. – pracownik Centrum Obsługi Informatycznej lub osoba zastępująca.
24. Osobą odpowiedzialną za realizację Umowy ze strony Wykonawcy jest *Pan/Pani*…….. lub osoba zastępująca.
25. Osobą odpowiedzialną za rozliczenie finansowe Umowy ze strony Zamawiającego jest pracownik Referatu ds. finansów i kontrolingu w Centrum Obsługi Informatycznej lub osoba go zastępująca.
26. *Środki finansowe w wysokości …… złotych (słownie: …… złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …… zostały ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……: Dz. ……., Rozdz. ……., § ……., zadanie ……., ……., ……. .*
27. *Środki finansowe w wysokości …… złotych (słownie: …… złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …… zostaną ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……: Dz. ……., Rozdz. ……., § ……., zadanie ……., ……., ……. .*

28. *Środki finansowe w wysokości …… złotych (słownie: …… złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …… zostaną ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……: Dz. ……, Rozdz. ……, § ……, zadanie ……, ……, …….* .
29. *Środki finansowe w wysokości …… złotych (słownie: …… złotych …/100) na realizację zaciągniętego zobowiązania finansowego w roku …… zostaną ujęte w planie finansowym Urzędu Miasta Krakowa na rok ……: Dz. ……, Rozdz. ……, § ……, zadanie ……, ……, …….* .
30. Po zakończeniu terminu obowiązywania Umowy, o którym mowa w § 2 ust. 2, Centrum Obsługi Informatycznej przekaże do Wydziału Finansowego Urzędu Miasta Krakowa pisemną informację potwierdzającą należyte wykonanie przedmiotu Umowy przez Wykonawcę.

§ 4

Kary umowne

1. Za niewykonywanie lub nienależyte wykonanie przedmiotu Umowy, o którym mowa w § 1 ust. 1, z przyczyn leżących po stronie Wykonawcy lub odstąpienie od niej przez którąkolwiek ze Stron, z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% łącznego wynagrodzenia brutto, o którym mowa w § 3 ust. 1.
2. Za niewykonywanie przedmiotu Umowy rozumie się zwłokę Wykonawcy w stosunku do terminu dostarczenia subskrypcji, określonego w § 1 ust. 2, przekraczającą 30 dni.
3. Za nienależyte wykonanie przedmiotu Umowy rozumie się w szczególności dostarczenie subskrypcji obarczonych wadami technicznymi lub prawnymi, dostarczenie subskrypcji innych niż wskazane w Umowie, termin obowiązywania subskrypcji inny niż wskazany w Umowie, zapewnienie Zamawiającemu dostępu do wadliwej konsoli chmurowej, świadczenie usług wsparcia technicznego w sposób niezgodny z zapisami Umowy.
4. Za zwłokę Wykonawcy w stosunku do terminu dostarczenia subskrypcji, określonego w § 1 ust. 2, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 1 000,00 złotych (słownie: jeden tysiąc złotych 00/100) za każdy dzień zwłoki.
5. Zamawiający naliczy Wykonawcy karę umowną w wysokości 300,00 zł (słownie: trzysta złotych 00/100, za każdy rozpoczęty dzień zwłoki, w przypadku zwłoki w zapłacie wynagrodzenia należnego podwykonawcy z tytułu zmiany wysokości wynagrodzenia, o której mowa w § 8 ust 5 pkt 6.
6. Zamawiający może odstąpić od Umowy do dnia upływu terminu obowiązywania umowy określonego w par. 1 ust. 2 Umowy, w przypadku gdy Wykonawca nie wykonuje lub nienależycie wykonuje przedmiot Umowy z przyczyn leżących po stronie Wykonawcy. Oświadczenie o odstąpieniu od Umowy ma skutek na ostatni dzień miesiąca i wywoła skutek ex tunc.
7. Zamawiający, korzystając z prawa umownego lub ustawowego odstąpienia od umowy, może zgodnie ze swoim wyborem odstąpić od całości Umowy lub od jej części. W przypadku, gdy Zamawiający odstąpi od części Umowy, skutek odstąpienia następuje na przyszłość, a Wykonawca zachowuje prawo do wynagrodzenia za wykonaną część przedmiotu Umowy do dnia wygaśnięcia Umowy na skutek odstąpienia.

8. Kary umowne naliczane są niezależnie i podlegają kumulacji, z zastrzeżeniem że:
   1) w przypadku, gdy zwłoka Wykonawcy, o której mowa w ust. 4 przekroczy 30 dni, Zamawiający nie naliczy kary umownej za zwłokę, o której zmowa w ust. 4, a naliczy karę umowną za niewykonywanie przedmiotu Umowy, o której mowa w ust. 1,
   2) w przypadku naliczenia Wykonawcy kary umownej z tytułu odstąpienia od Umowy, z przyczyn leżących po stronie Wykonawcy, których podstawą będzie niewykonywanie przez Wykonawcę przedmiotu Umowy lub nienależyte wykonanie Umowy, Zamawiający nie naliczy kary umownej za niewykonywanie/nienależyte wykonanie przedmiotu Umowy .
9. W przypadku niezłożenia przez Wykonawcę w wyznaczonym przez Zamawiającego terminie żądanych przez Zamawiającego dowodów, o których mowa w § 8 ust. 1, Zamawiający naliczy każdorazowo karę umowną w wysokości 500,00 zł (słownie: pięćset złotych 00/100) za każde rozpoczęte 7 dni zwłoki w przedstawieniu dowodów.
10. Łączna odpowiedzialność Wykonawcy z tytułu kar umownych nie przekroczy 50% wartości wynagrodzenia brutto, określonego w § 4 ust. 1 zdanie pierwsze.
11. Z zastrzeżeniem wyjątków wynikających z powszechnie obowiązujących przepisów prawa , Strony wyrażają zgodę na potrącenie – także przed terminem ich wymagalności – wierzytelności Zamawiającego z tytułu kary umownej z każdą wierzytelnością Wykonawcy wobec Zamawiającego, w tym z tytułu wynagrodzenia za realizację Umowy. Potrącenie jest skuteczne z chwilą złożenia Wykonawcy przez Zamawiającego oświadczenia o potrąceniu (potrącenie umowne).
12. Zastrzeżone w Umowie prawo odstąpienia od Umowy nie wyklucza możliwości skorzystania przez Wykonawcę z prawa odstąpienia od Umowy na podstawie powszechnie obowiązujących przepisów prawa.
13. Zapłata kary umownej przez Wykonawcę nie odbiera Kupującemu prawa do odstąpienia od Umowy.
14. Zamawiający może dochodzić na zasadach ogólnych odszkodowania przewyższającego wysokość kar umownych zastrzeżonych w Umowie, a także dochodzić wszelkich kar umownych również po wygaśnięciu Umowy.
15. Wykonawca wyraża zgodę na przesyłanie w formie elektronicznej, na adres: ……. *(np. e-doręczenia lub e-mail)*, not księgowych z tytułu naliczenia kar umownych.

§ 5

Klauzula Poufności

1. Strony zobowiązują się do zachowania w tajemnicy wobec osób trzecich informacji poufnych oraz do niewykorzystywania informacji poufnych dla celów innych aniżeli służące realizacji przedmiotu Umowy.
2. Za informacje poufne rozumie się wszelkie informacje lub materiały dotyczące Strony, stanowiące tajemnice prawem chronione, w tym informacje chronione na podstawie obowiązujących w Rzeczypospolitej Polskiej przepisów o ochronie danych osobowych i przepisów o ochronie informacji niejawnych, a także informacje powzięte lub otrzymane przez jedną Stronę od drugiej Strony w związku z wykonywaniem lub przy okazji

wykonywania przedmiotu Umowy, w stosunku do których Strona przekazująca zastrzegła ich poufny charakter.

3. Obowiązek ochrony informacji poufnych spoczywa na Stronie niezależnie od formy ich przekazania przez drugą Stronę, w tym w formie przekazu ustnego, dokumentu papierowego lub zapisu elektronicznego.
4. Obowiązek zachowania poufności nie dotyczy informacji, których ujawnienie jest wymagane przez powszechnie obowiązujące przepisy prawa lub które są powszechnie znane lub zostały podane do publicznej wiadomości przez Stronę uprawnioną lub za jej zezwoleniem.
5. Wykonawca nie będzie sporządzać kopii informacji poufnych Zamawiającego, z wyjątkiem kopii niezbędnych do realizacji przedmiotu Umowy. Wszelkie wykonane kopie będą określone jako należące do Zamawiającego.
6. Wykonawca nie będzie podejmował czynności mających na celu uzyskanie informacji poufnych Zamawiającego, innych aniżeli udostępnione przez Zamawiającego w celu realizacji przedmiotu Umowy.
7. Wykonawca może ujawnić informacje poufne Zamawiającego osobie trzeciej wyłącznie po uzyskaniu uprzedniej zgody Zamawiającego, wyrażonej na piśmie, pod rygorem uznania, że tego rodzaju zgoda nie została udzielona.
8. Wykonawca, po wykonaniu przedmiotu Umowy, z dniem zakończenia świadczenia usług na jej podstawie, zobowiązany jest do zwrotu wszystkich informacji poufnych Zamawiającemu, w tym sporządzonych kopii informacji poufnych Zamawiającego, a gdyby to nie było możliwe – do całkowitego i trwałego usunięcia informacji poufnych, chyba że szczególny przepis prawa stanowi inaczej. Nie dotyczy to informacji potrzebnych Wykonawcy do realizacji innych umów zawartych między Stronami do dnia ich wygaśnięcia.
9. Obowiązek zachowania w tajemnicy informacji poufnych spoczywa na Wykonawcy także przez 10 lat po wygaśnięciu Umowy, niezależnie od przyczyn wygaśnięcia, chyba że szczególny przepis prawa stanowi inaczej. Wykonawca zobowiązuje się do przekazania osobom, których to dotyczy, informacji o czasie trwania tego obowiązku.
10. Realizacja zobowiązań wynikających z postanowień niniejszego paragrafu wymaga od Wykonawcy zachowania należytej staranności, uwzględniającej profesjonalny charakter działania Wykonawcy. Wykonawca jest w pełni odpowiedzialny za każdą szkodę poniesioną przez Zamawiającego w związku z naruszeniem przez Wykonawcę postanowień niniejszego paragrafu.

§ 6

Podwykonawcy

1. Wykonawca może powierzyć wykonanie obowiązków umownych podwykonawcy/-om. *Podwykonawca/-y wykonywać będzie/-ą następujące części zamówienia (wskazanie podmiotu i części zamówienia, którą wykona ten podmiot/-y):*
   1) ……
   2) ……
2. Wykonawca ponosi odpowiedzialność za działanie lub zaniechanie podwykonawcy/-ów jak za działanie lub zaniechanie własne, w tym zakresie kar umownych. Niewykonanie lub nienależyte wykonanie przez podwykonawcę/-ów zobowiązań związanych z realizacją przedmiotu Umowy będzie traktowane

jako niewykonanie lub nienależyte wykonanie zobowiązań związanych z realizacją Umowy z przyczyn leżących po stronie Wykonawcy.

3. Wykonawca może powierzyć wykonanie obowiązków umownych podwykonawcy/-om w trakcie realizacji przedmiotu Umowy. Ust. 2 stosuje się odpowiednio. Wykaz ww. podmiotów oraz części zamówienia, które wykonają zostanie wprowadzony do Umowy aneksem.
4. *W przypadku, gdy Wykonawca składając ofertę w postępowaniu, o którym mowa w preambule, polegał będzie na zdolności technicznej i/lub zawodowej innych podmiotów na zasadach określonych w Dziale II Rozdziale 2 Oddział 3 ustawy Prawo zamówień publicznych, Wykonawca zobowiązany jest do wykonywania zamówienia z udziałem tych podmiotów. Podmioty te wykonywać będą następujące części zamówienia (wskazanie podmiotu i części zamówienia, którą wykona ten podmiot):*
   1) ……
   2) ……
5. Wykonawca ma prawo do zmiany podmiotów, o których mowa w ust. *1* i 3, *4* lub rezygnacji z wykonywania przez nich części zamówienia. W przypadku powierzenia wykonania obowiązków umownych nowemu podmiotowi, stosuje się odpowiednio zasady opisane w ust. 3.
6. *Jeżeli zmiana albo rezygnacja dotyczy podmiotu, o którym mowa w ust. 4, na którego zasoby Wykonawca powoływał się, w celu wykazania spełniania warunków udziału w postępowaniu, o którym mowa w preambule, Wykonawca jest obowiązany wykazać Zamawiającemu (przedkładając odpowiednie dokumenty, analogiczne do wymaganych w ogłoszeniu o zamówieniu w postępowaniu, o którym mowa w preambule), że proponowany inny podmiot lub wykonawca samodzielnie spełnia warunki udziału w postępowaniu w stopniu nie mniejszym niż podmiot, na którego zasoby Wykonawca powoływał się w trakcie postępowania o udzielenie zamówienia. Wykonawca zobowiązany jest wykazać także, że nie zachodzą - wobec proponowanego innego podmiotu - podstawy wykluczenia analogiczne do wymaganych w ogłoszeniu o zamówieniu w postępowaniu, o którym mowa w preambule. Jeżeli Zamawiający stwierdzi, że wobec proponowanego innego podwykonawcy zachodzą podstawy wykluczenia wskazane w postępowaniu, o którym mowa w preambule, wówczas Wykonawca zobowiązany jest zastąpić ten podmiot lub zrezygnować z powierzenia wykonania tej części zamówienia . Ust. 3 zdanie drugie i trzecie stosuje się odpowiednio*

§ 7

Elektromobilność

1. W przypadku wykorzystania przy realizacji zadania, o którym mowa w § 1 floty pojazdów samochodowych, Wykonawca oświadcza, że zapewni udział pojazdów elektrycznych lub pojazdów napędzanych gazem ziemnym we flocie pojazdów użytkowanych przy wykonywaniu Umowy zgodnie z wymogami określonymi w art. 68 ust. 3 ustawy z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych (Dz. U. z 2023 r. poz. 875 ze zm.). W takim przypadku Wykonawca zobowiązuje się na żądanie Zamawiającego poddać kontroli w celu potwierdzenia spełnienia tego wymogu, w szczególności Wykonawca zobowiązuję się przedłożyć na każde żądanie Zamawiającego – w terminie 14 Dni roboczych od otrzymania żądania - odpowiednie dokumenty, z których wynikać będzie spełnienie przez niego warunku wymagania określonego w zdaniu pierwszym, przykładowo: karty pojazdów i dowody rejestracyjne pojazdów używanych przy wykonywaniu Umowy i umów,

z których wynika prawo do dysponowania tymi pojazdami.

2. Obowiązek, o którym mowa w ust. 1 ma również zastosowanie w przypadku korzystania przez Wykonawcę przy wykonywaniu niniejszej Umowy z podwykonawców.
3. Przy obliczaniu udziału pojazdów, o którym mowa w ust. 1 stosuje się zasadę, zgodnie z którą wielkość tego udziału wynoszącą poniżej 0,5 zaokrągla się w dół, a wielkość tego udziału wynoszącą 0,5 i powyżej zaokrągla się w górę.
4. Przez pojazdy samochodowe, o których mowa w ust. 1 należy rozumieć pojazdy zdefiniowane w art. 2 pkt 33 ustawy z dnia 20 czerwca 1997 r. Prawo o ruchu drogowym (t.j. Dz. U. z 2023 r. poz. 1047 ze zm.), a przez pojazdy elektryczne i pojazdy napędzane gazem ziemnym, o których mowa w ust. 1 należy rozumieć pojazdy zdefiniowane w art. 2 odpowiednio pkt 12 i 14 ww. ustawy z dnia 11 stycznia 2018 r. o elektromobilności i paliwach alternatywnych.

§ 8

Postanowienia końcowe

1. Poza przypadkami wyraźnie przewidzianymi w Umowie, zmiany Umowy, a także oświadczenia o wypowiedzeniu lub odstąpieniu od Umowy, wymagają *zachowania formy pisemnej pod rygorem nieważności / formy elektronicznej z użyciem kwalifikowanego podpisu elektronicznego*, z zastrzeżeniem art. 455 ustawy Prawo zamówień publicznych. Zmiany, o których mowa w ust. 2 pkt 4 są dopuszczalne w formie dokumentowej.
2. Zmiany Umowy mogą wynikać w szczególności z następujących okoliczności:
   1) ze zmian powszechnie obowiązujących przepisów prawa w tym w szczególności:
      a) gdy w trakcie obowiązywania Umowy ulegnie zmianie stawka podatku od towarów i usług oraz podatku akcyzowego (na przedmiot Umowy); w takim przypadku zmianie ulegnie wysokość wynagrodzenia brutto Wykonawcy w ten sposób, iż zostanie ono powiększone lub zmniejszone o kwotę stanowiącą różnicę pomiędzy kwotą podatku według stawki obowiązującej w dniu zawarcia Umowy i kwotą podatku obliczoną według nowej stawki obowiązującej po wprowadzeniu zmiany w obowiązujących w tym zakresie przepisach prawa. Przedmiotowe postanowienie ma zastosowanie do tej części wynagrodzenia brutto Wykonawcy, do którego będzie miała zastosowanie zmieniona stawka podatku. W przypadku podatku od towarów i usług podstawą wyliczenia kwoty podatku będzie kwota ceny netto Wykonawcy, która nie ulegnie zmianie na skutek zmiany stawki tego podatku,
      b) zmiany wysokości minimalnego wynagrodzenia za pracę albo wysokości minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),
      c) zmiany zasad podlegania ubezpieczeniom społecznym lub ubezpieczeniu zdrowotnemu lub wysokości stawki składki na ubezpieczenia społeczne lub zdrowotne (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),
      d) zmiany zasad gromadzenia i wysokości wpłat do pracowniczych planów kapitałowych, o których

mowa w ustawie z dnia 4 października 2018 r. o pracowniczych planach kapitałowych (jeżeli zmiany te będą miały wpływ na koszty wykonania zamówienia przez Wykonawcę),

2) ze zmian cen materiałów lub kosztów związanych z realizacją zamówienia, stosownie do art. 439 ustawy Prawo zamówień publicznych,
3) zmiany podmiotów, o których mowa w § 6,
4) zmiany adresów korespondencyjnych, adresów e-mail lub danych osób odpowiedzialnych za realizację Umowy,
5) potrzeby zmiany terminów realizacji Umowy (w tym potrzeby zmiany terminu rozliczenia Umowy) z przyczyn niezależnych od Stron, jak również z przyczyn których Strony, działając z należytą starannością nie były w stanie przewidzieć. Przedłużenie terminu może nastąpić o czas niezbędny do wykonania właściwego zakresu przedmiotu Umowy, jednak nie dłużej niż o okres trwania przeszkody uniemożliwiającej wykonywanie przedmiotu Umowy. Zmiana terminu Umowy może być związana ze zmianą innych relewantnych zapisów Umowy. Strony zobowiązują się do wzajemnego powiadamiania o zaistnieniu powyższych okoliczności. Powiadomienia, o którym mowa w zdaniu poprzednim, należy dokonać co najmniej w formie dokumentowej, niezwłocznie po zaistnieniu ww. okoliczności. Do powiadomienia należy dołączyć dowody zaistnienia tych okoliczności.

3. Zmiany Umowy, o których mowa w ust. 2 pkt 3-5 nie mogą prowadzić do zwiększenia wysokości wynagrodzenia brutto określonego w § 3 ust. 1. Zmiany Umowy, o których mowa w ust. 2 pkt 1 i 2 mogą prowadzić do zwiększenia wysokości wynagrodzenia brutto określonego w § 3 ust. 1.
4. W przypadku zmian określonych w ust. 2 pkt 1 lit b-d Zamawiający dopuszcza możliwość waloryzacji wynagrodzenia brutto określonego w § 3 ust. 1 wyłącznie:
   1) na pisemny wniosek Wykonawcy,
   2) w zakresie niezrealizowanej części zamówienia,
   3) w oparciu o wykazaną, odpowiednimi dokumentami i dowodami, wartość wzrostu kosztów wykonania zamówienia (kosztów pracy personelu), i tylko w zakresie w jakim wykazany zostanie jej wpływ na wartość wynagrodzenia,
   4) najwcześniej od dnia wejścia w życie zmienionych przepisów, o ile wniosek wraz z dowodami zostanie złożony Zamawiającemu w terminie do 30 dni przed dniem wejścia w życie przepisów stanowiących podstawę zmiany. Nie dochowanie tego warunku spowoduje zmianę wynagrodzenia w terminie 30 dni od dnia złożenia wniosku wraz z dowodami.
5. W przypadku zmian określonych w ust. 2 pkt 2, Strony dopuszczają możliwość waloryzacji wynagrodzenia (poprzez jego wzrost lub obniżenie) określonego w § 3 ust. 1 - nie wcześniej jednak niż po upływie minimum 12 miesięcy realizacji Umowy - i wyłącznie:
   1) w przypadku zmiany poziomu cen materiałów lub kosztów związanych z realizacją zamówienia wynoszącej co najmniej 10 % w stosunku do poziomu cen z dnia zawarcia Umowy,
   2) na pisemny wniosek Wykonawcy lub Zamawiającego, stosownie do art. 439 ust. 4 ustawy Prawo zamówień publicznych,

3) w zakresie niezrealizowanej części zamówienia,
4) w oparciu o wykazaną, odpowiednimi dokumentami i dowodami, wartość zmiany cen materiałów lub kosztów związanych z realizacją zamówienia potwierdzoną wskaźnikiem cen producentów usług związanych z obsługą działalności gospodarczej dla działalności związanej z oprogramowaniem i doradztwem w zakresie informatyki oraz działalności powiązanej, ogłaszanym w komunikacie Prezesa Głównego Urzędu Statystycznego i tylko w zakresie w jakim wykazany zostanie ich wpływ na wartość wynagrodzenia umownego, o którym mowa w § 3 ust. 1,
5) maksymalnie o 15.% w stosunku do pierwotnego poziomu wynagrodzenia określonego w § 3 ust. 1, łącznie w całym okresie obowiązywania Umowy, przy czym jednorazowa waloryzacja wynagrodzenia nie może przekroczyć 5% wynagrodzenia o którym mowa wyżej,
6) z jednoczesną zmianą wynagrodzenia przysługującego podwykonawcy, z którym Wykonawca zawarł Umowę, w zakresie odpowiadającym zmianom cen materiałów lub kosztów dotyczących zobowiązania podwykonawcy, jeżeli łącznie spełnione są następujące warunki:
   a) przedmiotem Umowy podwykonawczej są roboty budowlane, dostawy lub usługi,
   b) okres obowiązywania Umowy podwykonawczej przekracza 6 miesięcy,
7) Strona, w terminie 30 dni od dnia złożenia wniosku, dokona jego oceny i podejmie decyzję o ewentualnej zmianie wysokości wynagrodzenia lub odmówi wprowadzania zmiany, przedstawiając swoje stanowisko (w termin ten nie wlicza się okresu pozyskania od drugiej strony dodatkowych wyjaśnień lub dokumentów),
8) najwcześniej po 21 dniach od złożenia wniosku, i nie wcześniej niż od płatności ceny za następny Rok rozliczeniowy dot. płatności ceny, o którym mowa w § 4 ust. 1, przy czym zmiany ceny nie mogą następować częściej niż co 12 miesięcy

6. W razie wystąpienia istotnej zmiany okoliczności powodującej, że wykonanie Umowy nie leży w interesie publicznym, dalsze wykonywanie Umowy może zagrozić podstawowemu interesowi bezpieczeństwa państwa lub bezpieczeństwu publicznemu czego nie można było przewidzieć w chwili zawarcia Umowy, Zamawiający może odstąpić od Umowy w terminie 30 dni od dnia powzięcia wiadomości o tych okolicznościach. W takim przypadku Wykonawca może żądać jedynie wynagrodzenia należnego mu z tytułu faktycznego wykonania części Umowy.
7. Przeniesienie na osobę trzecią wierzytelności Wykonawcy wynikających z Umowy wymaga zgody Prezydenta Miasta Krakowa wyrażonej na piśmie pod rygorem nieważności, z zastrzeżeniem zachowania zarzutów przeciwko zbywcy wierzytelności.
8. W sprawach nieuregulowanych Umową, a także w sprawach zobowiązań wynikających z Umowy, wyłączne zastosowanie mają powszechnie obowiązujące przepisy prawa polskiego.
9. Wyłączną jurysdykcję w sprawach rozstrzygania sporów i spraw związanych z Umową sprawują sądy polskie. Strony zrzekają się prawa do kwestionowania właściwości tych sądów. W ramach jurysdykcji, o której mowa w zdaniu pierwszym, Strony poddają się rozstrzygnięciom sądu powszechnego właściwego miejscowo dla siedziby Zamawiającego.

10. W przypadku, gdy którekolwiek z postanowień Umowy, z mocy prawa lub prawomocnego orzeczenia jakiegokolwiek organu lub sądu, zostaną uznane za nieważne lub bezskuteczne, pozostałe postanowienia Umowy zachowują ważność i skuteczność.
11. Za datę zawarcia Umowy Strony uznają dzień złożenia *kwalifikowanego podpisu elektronicznego przez ostatnią spośród osób reprezentujących Strony / podpisu przez ostatnią spośród osób reprezentujących Strony*.
12. Załączniki wymienione w Umowie stanowią jej integralną część.
13. Umowę z **……**, której przedmiotem jest ……, sporządzono *w formie pisemnej pod rygorem nieważności, w dwóch jednobrzmiących egzemplarzach, jeden dla Zamawiającego, jeden dla Wykonawcy i podpisano z użyciem własnoręcznych podpisów / w formie elektronicznej i podpisano przy użyciu kwalifikowanych podpisów elektronicznych*.

Załączniki:

1) Załącznik nr 1 do Umowy – Wymagania Oprogramowania
2) Załącznik nr 2 do Umowy - Raport - Rozliczenie czasu wsparcia technicznego

Treści we wzorze Umowy zapisane kursywą znajdą się w Umowie zawieranej z Wykonawcą, jeżeli będą adekwatne do sytuacji przedmiotowej i podmiotowej tego Wykonawcy.

ZAMAWIAJĄCY	**WYKONAWCA**
Imię Nazwisko *Funkcja podpisującego*	***Imię Nazwisko*** *Funkcja podpisującego*
Imię Nazwisko *Funkcja podpisującego*	***Imię Nazwisko*** *Funkcja podpisującego*

Dokument podpisano z użyciem podpisów elektronicznych.

Załącznik nr 1 do Umowy

Definicje

1. **APT** - Advanced Persistent Threats - zaawansowane cyberzagrożenia powiązane z działalnością samodzielnych zorganizowanych grup cyber przestępczych lub grup cyber przestępczych sponsorowanych przez państwa.
2. **Endpoint** - stacje robocze użytkowników oraz serwery.
3. **Exploit** - plik z danymi lub dane przesłane w ruchu sieciowym skonstruowane w sposób umożliwiający wykorzystanie (wyeksploitować) luki bezpieczeństwa w oprogramowaniu otwierającym plik lub odbierającym dane i docelowo mające doprowadzić do przejęcia kontroli nad Endpointem.
4. **SaaS** - Software as a Service - system (aplikacja) dostarczana przez producenta w formie gotowej do wykorzystania usługi bez konieczności utrzymywania infrastruktury po stronie użytkownika. Do dostarczania aplikacji w formie SaaS wykorzystywane są usługi dostawców chmury publicznej co oznacza, że dane są przetwarzane i przechowywane poza ośrodkami przetwarzania danych użytkownika systemu. W tym modelu dostawca oprogramowania odpowiada za utrzymanie dostępności systemu zgodnie z wymogami z określonymi w umowie oraz za jego aktualizację.

Wymagania Oprogramowania

1. Oprogramowanie musi być dostarczone w formie SaaS, a zebrane logi muszą być przechowywane i przetwarzane (włącznie z sandboxingiem) na terenie Polski a producent Oprogramowania musi posiadać certyfikację SOC 2 Type 2 (procedura audytowa, której efektem jest raport szczegółowo opisujący w jaki sposób dostawca usług zarządza powierzonymi mu danymi - opisuje system zarządzania bezpieczeństwem informacji i ocenia jego adekwatność w kontekście punktów kontrolnych standardu) oraz gwarantować dostępność usługi na poziomie 99,9%.
2. Dokumentacja Oprogramowania musi być publikowana przez producenta na jego stronie internetowej co najmniej w języku angielskim.
3. Oprogramowanie musi przechowywać informacje o alarmach i incydentach włącznie z grafami przyczynowo skutkowymi co najmniej przez 180 dni.
4. Oprogramowanie musi przechowywać szczegółowe dane telemetryczne z Endpointów zabezpieczonych agentem przez co najmniej 30 dni.
5. Oprogramowanie musi szyfrować dane w trakcie transmisji i w trakcie przechowywania za pomocą protokołów i algorytmów kryptograficznych uznanych powszechnie za bezpieczne. Producent Oprogramowani musi zagwarantować, że dostęp do przechowywanych danych posiada tylko i wyłącznie producent i że dostęp do danych nie jest możliwy dla żadnej trzeciej strony. Dane w trakcie przechowywania muszą być szyfrowane algorytmem AES-256.

6. Oprogramowanie wg ewaluacji MITRE Engenuity: Mitre Attack (https://attackevals.mitre-engenuity.org/enterprise/wizard-spider-sandworm/) musi posiadać skuteczność na poziomie minimum 95% w następujących kategoriach:
    a) widoczności zagrożeń (sekcja Visibility)
    b) analityki zagrożeń (sekcja Analytics Coverage)
7. Oprogramowanie musi umożliwiać zarządzania przez pojedynczy webowy interfejs graficzny z wykorzystaniem graficznej przeglądarki internetowej oraz przez API. Oba muszą być dostępne po https (co najmniej TLS 1.2). Nie dopuszcza się, aby webowy interfejs graficzny korzystał z technologii flash, silverlight lub java.
8. Wszystkie składniki Oprogramowania muszą być konfigurowalne i zarządzane przez jeden spójny interfejs. Nie dopuszcza się, aby składniki Oprogramowania posiadały oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On).
9. Wymagana jest ocena na poziomie min „A+" dla wszystkich serwisów, z których korzysta oferowane Oprogramowanie. Ocena będzie weryfikowana przy pomocy ogólnodostępnego narzędzia https://www.ssllabs.com
10. Oprogramowanie musi posiadać możliwość ograniczenia logowania do Oprogramowania tylko ze wskazanych publicznych adresów IP.
11. Oprogramowanie musi umożliwiać integrację z zewnętrznym katalogiem użytkownik via SAML 2.0 (ze wsparciem dla ADFS) oraz posiadać możliwość definiowania lokalnych użytkowników, których logowanie jest zabezpieczone hasłem oraz dodatkowym czynnikiem uwierzytelniającym w formie tokenu. Oprogramowanie jako dodatkową metodę uwierzytelnienia musi wspierać tokeny w formie jednorazowych kodów generowanych w aplikacji mobilnej wg. algorytmu Time-based One-Time Password algorithm (ang. TOTP-based). Wymaga się zastosowania Google Authenticator lub Microsoft Authenticator na platformy Android i iOS dla aplikacji mobilnej służącej jako dodatkowa metoda uwierzytelnienia.
12. Oprogramowanie dla lokalnych kont podczas tworzenia haseł dla kont administracyjnych musi żądać stosowania się do przyjętej polityki, która wymaga ustawienia hasła spełniającego następujące kryteria: co najmniej 11 znaków, musi zawierać małe i duże litery łacińskie, cyfry i znaki specjalne.
13. Oprogramowanie musi umożliwiać przypisywanie użytkowników do grup użytkowników. Dodatkowo w przypadku użytkowników uwierzytelnionych via SAML 2.0 musi istnieć możliwość zmapowania grup SAML do lokalnie zdefiniowanych grup.
14. Każdy użytkownik Oprogramowania (administrator, operator, analityk) muszą posiadać indywidualne konta pozwalające na jego jednoznaczną identyfikację.
15. Oprogramowanie musi umożliwiać określenie zakresu dostępu z wykorzystaniem ról i ich przypisanie do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego Oprogramowania, jego rodzaju (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane Endpointy).

16. Oprogramowania w ramach roli musi umożliwiać określenie dostępu do co najmniej następujących obszarów:
    a) Ustawienia Oprogramowania
    b) Zarządzanie Endpointami
    c) Zarządzanie politykami
    d) Zarządzanie regułami detekcyjnymi
    e) Zarządzania wykluczeniami
    f) Zarządzanie incydentami
    g) Uruchamianie odpowiedzi na incydent
    h) Nawiązywanie połączenia do linii poleceń
    i) Uruchamianie skryptów python
    j) Zarządzanie kwerendami do danych
    k) Zarządzanie raportami
    l) Zarządzenie dashboardami/kokpitami
17. Oprogramowanie musi posiadać możliwość definiowania własnych dopasowanych do potrzeb ról.
18. Oprogramowanie musi posiadać zestaw dashboardów informujących co najmniej:
    a) O liczbie i powadze incydentów incydentów
    b) O liczbie incydentów przypisanych do analityków
    c) O hostach z największą liczbą incydentów
    d) O liczbie agentów z rozbiciem na wersję agenta
    e) O liczbie agentów z rozbiciem na agentów offline i online
    f) O liczbie agentów z rozbiciem na wersję aktualizacji podsystemów bezpieczeństwa
    g) O liczbie agentów z rozbiciem na status ochrony
19. Oprogramowanie musi umożliwiać tworzenie własnych spersonalizowanych dashboardów z wykorzystaniem predefiniowanych kontrolek/widgetów oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych.
20. Oprogramowanie musi umożliwiać skonfigurowanie okresu czasu, po którym użytkownik zostanie automatycznie wylogowany z Oprogramowania oraz możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni.
21. Oprogramowanie musi co najmniej przez 365 dni przechowywać logi audytowe dokumentujące akcje podejmowane przez użytkowników zalogowanych do Oprogramowania oraz logi audytowe dotyczące funkcjonowania agentów.
22. Oprogramowanie musi posiadać możliwość eksportu wybranych logów audytowych via syslog po ssl/tls w formacie CEF. W dokumentacji Oprogramowania musi być wskazany adres IP lub zakres adresów IP, z których nawiązywane będzie połączenie syslog.
23. Oprogramowanie musi posiadać możliwość alarmowania o wskazanych zdarzeniach zapisanych w logach audytowych poprzez wysłanie emaila na wskazane skrzynki poczty elektronicznej.

24. Oprogramowanie musi posiadać możliwość integracji z Microsoft Active Directory w zakresie synchronizacji struktury organizacyjnej katalogu AD zarówno z lokalnym AD jak również z Azure AD na potrzeby automatycznego wzbogacania informacji na temat Endpointów i użytkowników oraz tworzenia dynamicznych grup Endpointów celem różnicowania konfiguracji agentów.
25. Oprogramowanie po integracji z Active Directory, musi mieć możliwość wyświetlenia widoku wszystkich komputerów obsługiwanych przez Active Directory Zamawiającego z możliwością filtrowania per OU. Konsola zarządzająca oferowanego rozwiązania musi wykrywać serwery będące członkami domeny Active Directory, na których nie zainstalowano agenta Oprogramowania. Widok powinien być podzielony na maszyny chronione i nie chronione przez agenta. Oprogramowanie co najmniej raz na dobę musi alarmować (co najmniej notyfikacja emailowa i via syslog), jeśli serwery w określonym OU nie są chronione przez agenta.
26. Oprogramowanie musi posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową.
27. Oprogramowanie musi posiadać oprogramowanie agenta co najmniej dla następujących systemów operacyjnych:
    a) Windows 7, 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)
    b) Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,
    c) Linux
        i. Red Hat Enterprise Linux 7, 8 i 9
        ii. Rocky Linux 8 i 9
        iii. SUSE Linux Enterprise Server 11, 12 i 15
        iv. Ubuntu 18.04 LTS, 20.04 LTS i 22.04 LTS
        v. Oracle Linux 6 i 7
        vi. CentOS 6,7 i 8
        vii. Debian 9, 10 i 11
    d) macOS 11.x, 12.x i 13.x
    e) Android 10,11 i 12
    f) iOS 15.x i 16.x
28. Oprogramowanie musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
    a) W formacie msi dla systemów Windows
    b) W formacie rpm, deb i sh dla systemów Linux
    c) W formacie pkg dla systemów macOS
    d) W formacie helm dla klastrów kubernetes
29. Pakiet instalacyjny agenta dla systemów Windows, macOS, Linux i klastrów kubernetes musi posiadać możliwość:

a) Przypisanie do Endpointa nieusuwalnego znacznika, który może być wykorzystany do tworzenia dynamicznych grup Endpointów i określenia zakresu dostępu jaki posiada rola użytkownika.
b) Skonfigurowania komponentu pośredniczącego w komunikacji z siecią rozległą
c) Wyłączenia opcji wykonywania skryptów python
d) Wyłączenia opcji pobierania plików
e) Wyłączenia opcji dostępu do linii poleceń

30. Pakiet instalacyjny agenta dla systemów Windows musi posiadać możliwość wskazania lokalnej kopii aktualizacji podsystemów bezpieczeństwa.
31. Instalacja agenta i jego aktywacja w systemie nie może wymagać restartu systemu operacyjnego.
32. Komunikacja pomiędzy agentem a serwerem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2) i w zależności od konfiguracji być realizowana w sposób bezpośredni lub pośredni via dedykowany komponent pośredniczący (dalej proxy) tego samego producenta, który:
    a) musi umożliwiać uruchomienie w formie maszyny wirtualnej
    b) musi obsługiwać funkcję proxy chaining dla http z uwierzytelnieniem
    c) musi umożliwiać cache'owanie aktualizacji oprogramowania agenta i aktualizacji podsystemów bezpieczeństwa agenta
33. Komunikacja pomiędzy proxy a Oprogramowaniem musi być zabezpieczona z wykorzystaniem https (co najmniej TLS 1.2). Proxy musi posiadać możliwość manualnej lub automatycznej aktualizacji. Oprogramowanie musi umożliwiać centralne zarządzanie ustawieniami proxy.
34. Oprogramowanie musi obsługiwać co najmniej 3 proxy.
35. W dokumentacji Oprogramowania muszą być wskazane publiczne adresy IP oraz adresy URL niezbędne do zapewnienia poprawnej komunikacji między agentami i Oprogramowania oraz pomiędzy proxy a Oprogramowaniem. Komunikacja musi być zawsze nawiązywana w kierunku od agenta/proxy do Oprogramowania.
36. Oprogramowanie musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup Endpointów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie:
    a) Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja
    b) Maksymalnej liczby równolegle aktualizowanych agentów
    c) Zakresu: tylko minor release, tylko minor release w ramach wskazanego major release, najnowszy major.minor release, najnowszy przedostatni major.minor release
    d) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowej wersji
    e) Źródła: bezpośrednio z Oprogramowania, z komponentu pośredniczącego, peer-to-peer
37. Oprogramowanie musi posiadać możliwość skonfigurowania manualnej i automatycznej różnicowej aktualizacji podsystemów bezpieczeństwa agenta dla wskazanych grup Endpointów. Polityka automatycznej aktualizacji podsystemów bezpieczeństwa musi umożliwiać określenie:
    a) Zakresu: tylko major release, najnowszy major.minor release
    b) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowego release

c) Źródła: bezpośrednio z Oprogramowania, z komponentu pośredniczącego, peer-to-peer
d) Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z Oprogramowania

38. Oprogramowanie musi umożliwiać alarmowanie w przypadku, gdy:
    a) Podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie
    b) Agent zostanie odinstalowany
    c) Agent nie zgłosi się od Oprogramowania a równocześnie Endpoint zaloguje się w domenie Active Directory (dotyczy systemów Windows)
39. Oprogramowanie musi umożliwiać różnicowanie konfiguracji agenta i podsytemów bezpieczeństwa poprzez przypisanie różnych profili konfiguracyjnych do wybranych grup Endpointów lub pojedynczych Endpointów.
40. Wszystkie dane telemetryczne muszą być przechowywane przez Oprogramowanie w centralnym i przeszukiwalnym repozytorium danych.
41. Oprogramowanie musi umożliwiać przeszukiwanie danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Reguły tworzenia kwerend muszą być opisane w dokumentacji Oprogramowania.
42. Oprogramowania musi umożliwiać zapisanie kwerendy do danych telemetrycznych do prywatnej biblioteki kwerend danego użytkownika lub do globalnej biblioteki kwerend dostępnej dla wszystkich innych użytkowników.
43. Oprogramowanie musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via REST API.
44. Oprogramowanie musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego.
45. Oprogramowanie musi umożliwiać uruchamianie kwerendy cyklicznie zgodnie z podanym harmonogramem lub jeden raz o określonym czasie.
46. Oprogramowanie musi umożliwiać wizualizację wyników kwerendy do danych telemetrycznych w formie tabelarycznej i w formie wykresu: liniowego, słupkowego i kołowego.
47. Oprogramowanie musi umożliwiać wykorzystanie wyników kwerendy do tworzenia periodycznie generowanych raportów.
48. Oprogramowanie musi umożliwiać wykorzystanie wyników kwerend do wizualizacji danych w dashboardach.
49. Oprogramowanie musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z zadanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła jakiekolwiek rekordy.
50. Oprogramowanie musi umożliwiać definiowanie atomowych wskaźników kompromitacji w formie: SHA256, nazwy domenowej, adresu IPv4, adresu IPv6, ścieżki, nazwy pliku. Musi istnieć możliwość dodania znacznika ręcznie, zaimportowania znaczników z pliku i via REST API oraz oznaczenia reputacji, wiarygodności i okresu wygaśnięcia znacznika.

51. Oprogramowanie musi umożliwiać definiowanie złożonych wskaźników kompromitacji opisujących zachowanie procesu co najmniej w zakresie: operacji plikowych, uruchamianych procesów i ich parametrów, operacji sieciowych i operacji na rejestrze (tylko windows).
52. Oprogramowanie dla każdego wprowadzonego atomowego i złożonego wskaźnika kompromitacji musi wygenerować alarm(-y):
    a) jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)
    b) jeśli znacznik zostanie odszukany w nowych danych telemetrycznych
53. Oprogramowanie musi umożliwiać przekształcanie złożonych wskaźników kompromitacji w reguły prewencyjne co najmniej dla agenta dla Windows, macOS i Linux.
54. Oprogramowanie musi umożliwiać integrację z VirusTotal.
55. Oprogramowanie musi umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych o określonych SHA256.
56. Oprogramowanie w ramach odpowiedzi na incydent musi umożliwiać:
    a) Remediację ze wskazaniem kroków, które mogą być podjęte automatycznie i kroków, które należy zrealizować manualnie. Musi istnieć możliwość wyboru kroków remediacyjnych, które zostaną wykonane automatycznie.
    b) Uruchomienie skryptu python na Endpointcie.
    c) Nawiązanie interaktywnego połączenia do linii poleceń na Endpoitcie.
    d) Wstrzymanie procesu na Endpointcie.
    e) Wyłączenie procesu na Endpoincie
    f) Izolację sieciową Endpointa.
    g) Dodanie adresu IP do listy publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.
    h) Dodanie nazwy domenowej do publikowanej po https z uwierzytelnieniem w celu integracji z firewallami i innymi systemami bezpieczeństwa.
    i) Zmianę w rejestrze (tylko systemy Windows).
    j) Usunięcie pliku na Endointcie.
    k) Przeniesienie pliku na Endpointcie do kwarantanny.
    l) Wyszukanie pliku na innych Endpointach
    m) Zrzucenie pamięci procesu na Endpointcie.
57. Oprogramowanie musi obsługiwać co najmniej następujące poziomy powagi alarmów: informacyjny, niski, średni, wysoki i krytyczny.
58. Oprogramowanie musi automatycznie grupować powiązane alarmy w celu przyspieszenia i ułatwienia triażu i analizy incydentu.
59. W ramach incydentu Oprogramowanie musi grupować:
    a) Powiązanych z incydentem użytkowników

b) Endpointy
c) Pliki
d) Domeny
e) Adresy IP

60. Oprogramowanie dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, tak aby analityk mógł w łatwy sposób przeanalizować wykorzystywane techniki, określić zakres ataku, ustalić potencjalny cel ataku i zweryfikować czy cel został osiągnięty.
61. Oprogramowanie musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport tego raportu.
62. Oprogramowanie musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
    a) Przypisanie incydentu do analityka
    b) Zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy
    c) Dodawanie notatek
    d) Komunikacja z innymi analitykami
    e) Raportowanie czasu MTTR
63. Oprogramowanie musi mapować alarmy do matrycy technik i taktyk MITRE ATT&CK.
64. Oprogramowanie musi zapewniać widoczność w czasie rzeczywistym podatności oraz aktualne poziomy poprawek na stacjach końcowych Linux i Windows wraz z aktualnymi informacjami o powadze dostarczone przez NIST National Vulnerability Database i Microsoft Security Response Center, w tym Common Vulnerabilities and Exposures (CVE).
65. Oprogramowanie musi zapewniać minimum widoczność informacji zebranych ze stacji końcowych na temat: użytkowników, grup, aplikacji, usług, sterowników, usług automatycznego uruchamiania, udziałów, dysków.
66. Agent dla systemów Windows:
    a) Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:
        i. Bezpośrednio z Oprogramowania
        ii. Z komponentu pośredniczącego
        iii. Od innych Endpointów w tej samej podsieci (peer-to-peer)
    b) Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa Endpointów lub indywidualnie dla danego Endpointa po stronie Oprogramowania. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym Oprogramowania.
    c) Musi być procesem chronionym w trybie PPL dla oprogramowanie anty-malware'owego.

d) Musi posiadać sterownik ELAM (Early Launch Anti-Malware).

e) Musi umożliwiać:

   i. Ukrycie ikony agenta w zasobniku systemowym
   ii. Wyłączenie powiadomień o zablokowanych zagrożeniach
   iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej
   iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego
   v. używanie komunikatów i powiadomień w języku polskim
   vi. Zarządzanie host firewallem Endpointa z wykorzystaniem Windows Filtering Platform
   vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu
   viii. Weryfikację stanu szyfrowania dysków
   ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte
   x. Usuwanie plików po SHA256 i po ścieżce

f) Musi posiadać możliwość wykonywania periodycznego skanowania Endpointu w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.

g) Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, base64, certifi, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, pytest, python_hosts, pythoncom, pytsk3, pywin32, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib.

h) Musi integrować się z Windows Security Center

i) Musi posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.

j) Musi posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w systemie plików.

k) Musi posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.

l) Do kolekcji danych telemetrycznych musi używać sterownika lub sterowników (działać w jądrze systemu operacyjnego).

m) Musi posiadać możliwość zrzucenia pamięci systemu operacyjnego
n) Musi posiadać możliwość zebrania historii przeglądarek internetowych
o) Musi posiadać możliwość wglądu w tablicę MFT (Master File Table) systemu plików
p) Musi wykonywać:
    i. monitoring zdarzeń w trybie kernela, aby uniemożliwić usunięcie hooków z poziomu programów działających w trybie użytkownika, co najmniej w następującym zakresie:
        1. Pobieranie informacji o procesach (tworzenie procesu i otwieranie handlerów)
        2. Pobieranie informacji o wątkach (tworzenie wątku i otwieranie handlerów)
        3. Pobieranie informacji o ładowaniu bibliotek dll
        4. Pobieranie informacji o próbach dostępu do rejestru
        5. Pobieranie informacji o operacjach na systemie plików.
    ii. monitoring co najmniej następujących funkcje NT API:
        1. VirtualAlloc i VirtualAllocEx
        2. VirtualProtect i VirtualProtectEx
        3. CreateThread, CreateRemoteThread i CreateRemoteThreadEx
        4. NtAllocateVirtualMemory i ZwAllocateVirtualMemory
        5. NtCreateThread, NtCreateThreadEx, ZwCreateThread i ZwCreateTheadEx
        6. NtProtectVirtualMemory i ZwProtectVirtualMemory
        7. NtSetInformationProcess i ZwSetInformationProcess
    iii. Monitoring zdarzeń ETW-TI (Event Tracing for Windows - Threat Intelligence) poprzez subskrypcję na zdarzenia Microsoft-Windows-Threat-Intelligence.
q) Musi zbierać i wysyłać do Oprogramowania co najmniej następujące dane telemetryczne:
    i. Utworzenie nowego procesu i zakończenie procesu
    ii. Wszystkie operacje na plikach: tworzenie, zapisywanie, kasowanie, zmiana nazwy, przesunięcie, modyfikacja, link symboliczny
    iii. Ładowanie bibliotek DLL
    iv. Wstrzykiwanie do procesu
    v. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, create, listen, close, bind
    vi. Statystyki połączeń sieciowych
    vii. Praca z rejestrem: skasowanie wartości, ustawienie wartości, utworzenie klucza, kasowanie klucza, zmiana nazwy klucza
r) Musi wysyłać zgromadzone dane telemetryczny do Oprogramowania nie rzadziej niż co 5 minut. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do Oprogramowania po przywróceniu łączności sieciowej.

s) Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:
    i. Przekierowanie APC
    ii. Obejście Data Execution Prevention
    iii. DLL Hijacking
    iv. Exploit Kit Fingerprinting
    v. JIT
    vi. Null Dereference
    vii. ROP
    viii. Structures exception handler hijackings
    ix. Heap Spray
    x. Kernel Privilege Escalation
t) Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:
    i. Weryfikacja sha256 w bazie threat intelligence producenta Oprogramowania
    ii. Analiza dynamiczna w sandboxie chmurowym producenta Oprogramowania (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście)
    iii. Lokalna analiza statyczna
    iv. Weryfikacja podpisu pliku binarnego
    v. Przeniesienie pliku binarnego do kwarantanny
    vi. Zablokowanie uruchomienia/załadowania złośliwego pliku binarnego
    vii. Zablokowanie uruchomienia pliku z przenośnej pamięci masowej USB
    viii. Zablokowanie uruchomienia pliku z innych lokalizacji sieciowych niż wskazane
    ix. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
    x. Wykrywanie shellcodu'u ładowanego do pamięci
    xi. Wykrycie i przerwanie próby szyfrowania plików na dysku (ochrona przeciw ransomware).
u) Musi wykrywać i blokować próbę wyłączenia Volume Shadow Copy Service (VSS).
v) Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy:
    i. Weryfikacja sha256 w bazie threat intelligence producenta Oprogramowania
    ii. Analiza dynamiczna w sandboxie chmurowym producenta Oprogramowania (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście)
    iii. Lokalna analiza statyczna

w) Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

x) Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.

y) Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy Endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.

67. **Agent dla systemów macOS:**

a) Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:

i. Bezpośrednio z Oprogramowania

ii. Z komponentu pośredniczącego

iii. Od innych Endpointów w tej samej podsieci (peer-to-peer)

b) Musi posiadać mechanizm ochronny przed nieautoryzowanymi próbami wyłączenia agenta nawet przez użytkowników z uprawnieniami administratora. Wyłączenie podsystemów bezpieczeństwa i odinstalowanie agenta musi wymagać podania hasła, które może być skonfigurowane per grupa Endpointów lub indywidualnie dla danego Endpointapo stronie Oprogramowania. Nie dopuszcza się rozwiązań, w których hasło jest statyczne i podawana w trakcie uruchamiania instalatora. Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym Oprogramowania.

c) Musi umożliwiać:

i. Ukrycie ikony agenta w zasobniku systemowym

ii. Wyłączenie powiadomień o zablokowanych zagrożeniach

iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej

iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego

v. Spolszczenie komunikatów powiadomień

vi. Zarządzanie host firewallem Endpointa

vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu

viii. Weryfikację stanu szyfrowania dysków

ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte

x. Usuwanie plików po SHA256 i po ścieżce

d) Musi posiadać możliwość wykonywania periodycznego skanowania Endpointu w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.

e) Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, base64, certifi, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, pytest, python_hosts, pythoncom, pytsk3, pywin32, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib.

f) Musi zbierać i wysyłać do Oprogramowania co najmniej następujące dane telemetryczne:
   i. Utworzenie nowego procesu i zakończenie procesu
   ii. Wszystkie operacje na socketach sieciowych dla TCP i UDP: accept, connect, connect failure, disconnect, listen.
   iii. Statystyki połączeń sieciowych

g) musi wysyłać zgromadzone dane telemetryczny do Oprogramowania nie rzadziej niż co 5 minut. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do Oprogramowania po przywróceniu łączności sieciowej.

h) Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:
   i. Dylib Hijacking
   ii. JIT
   iii. ROP

i) Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
   i. Weryfikacja sha256 w bazie threat intelligence producenta Oprogramowania
   ii. Analiza dynamiczna w sandboxie chmurowym producenta Oprogramowania (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście)
   iii. Lokalna analiza statyczna
   iv. Weryfikacja podpisu pliku binarnego
   v. Przeniesienie pliku binarnego do kwarantanny

vi. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego

j) Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

k) Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacja sieciowa) poza połączeniem do systemu.

l) Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy Endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez Oprogramowanie nie rzadziej niż co dwa tygodnie.

68. **Agent dla systemów Linux i klastrów kubernetes:**

a) Musi posiadać możliwość pobierania aktualizacji agenta i aktualizacji podsystemów bezpieczeństwa:

i. Bezpośrednio z systemu

ii. Z komponentu pośredniczącego

iii. Od innych Endpointów w tej samej podsieci (peer-to-peer)

b) Operacja deinstalacji agenta i wyłączenia podsystemów bezpieczeństwa musi zostać zapisana w dzienniku audytowym systemu.

c) Musi posiadać wsparcie dla rozszerzenia eBPF.

d) Musi posiadać możliwość wykonywania periodycznego skanowania Endpointu w zakresie zainstalowanych aplikacji, automatycznie uruchamiających się aplikacji, dysków, użytkowników, grup użytkowników i przypisania użytkowników do grup oraz zestawienia tych danych z wynikami poprzednich skanów.

e) Musi posiadać wbudowany runtime python 3.7 lub nowszy i możliwość uruchamiania wbudownych i własnych skryptów python z wykorzystaniem co najmniej następujących bibliotek: argparse, base64, certifi, contextlib, csv, ctypes, datetime, enum, fnmatch, functools, glob, globmatch, gzip, hashlib, importlib, io, json, LnkParse3, locale, logging, multiprocessing, netifaces, os, pathlib, pefile, platform, pprint, protobuf, psutil, pysftp, pytest, python_hosts, pythoncom, pytsk3, pywin32, pywintypes, queue, random, re, Registry, requests, runpy, setuptools, shlex, shutil, signal, socket, sqlite_utils, sqlite3, ssl, stat, struct, subprocess, sys, threading, time, traceback, types, unicodecsv, websocket, win32api, win32com, win32con, win32evtlog, win32evtlogutil, win32file, win32net, win32netcon, win32process, win32security, win32service, win32serviceutil, win32timezone, winerror, winreg, wmi, xml, xmljson, yara, zipfile, zlib.

f) Musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:

i. Utworzenie nowego procesu i zakończenie procesu

ii. Informacje o kontenerach
iii. Wszystkie operacje na socketach sieciowych dla TCP i UDP: listen, accept, connect, connect failure, disconnect

g) Musi wysyłać zgromadzone dane telemetryczny do systemu nie rzadziej niż co 5 minut. Jeśli z powodu braku łączności sieciowej agent nie może wysłać danych telemetrycznych, to dane telemetryczne muszą zostać lokalnie przechowane (zcache'owane) i wysłane do Oprogramowania po przywróceniu łączności sieciowej.

h) Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technika eksploitacji:
i. Java Deserialization
ii. SO Hijacking
iii. Heap spray
iv. ROP
v. Kernel Privilege Escalation

i) Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Oprogramowania
ii. Analiza dynamiczna w sandboxie chmurowym producenta Oprogramowania (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym hoście)
iii. Lokalna analiza statyczna
iv. Przeniesienie pliku binarnego do kwarantanny
v. Weryfikację i wykrycie groźnego zachowania procesu powstałego w wyniku uruchomienia/załadowania pliku binarnego
vi. Wykrywanie webshelli

j) Musi zapewnić ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w groźny sposób poprzez analizę złożonych łańcuchów przyczynowo-skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców.

k) Musi umożliwiać zablokowanie całego ruchu sieciowego (izolacji sieciowej) poza połączeniem do systemu.

l) Musi posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z systemem. Wyłączenie izolacji sieciowej musi być zabezpieczone hasłem. Każdy Endpoint musi posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło musi być automatycznie rotowane przez system nie rzadziej niż co dwa tygodnie.

69. **Agent dla systemów Android:**

a) Musi umożliwiać automatyczną instalację via system MDM i manualną via Google Play.

b) Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym systemu i wygenerować alarm.
c) Musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi aplikacjami wykorzystując co najmniej następujące mechanizmy:
    i. Weryfikacja sha256 w bazie threat intelligence producenta Oprogramowania
    ii. Analiza dynamiczna w sandboxie chmurowym producenta Oprogramowania

70. **Agent dla systemów iOS:**
a) Musi umożliwiać automatyczną instalację via system MDM i manualną via App Store.
b) Operacja deinstalacji agenta musi zostać zapisana w dzienniku audytowym Oprogramowania i wygenerować alarm.
c) Musi weryfikować i raportować integralność systemu operacyjnego (tzw. jail break).
d) Musi zapewniać ochronę przed groźnymi wiadomościami tekstowymi przez weryfikację linków url (ochrona przeciw smishingowa).
e) Musi zapewniać ochronę przed groźnymi połączeniami głosowymi (ochrona przeciw vishingowa).
f) Musi umożliwiać użytkownikowi raportowanie podejrzanych wiadomości tekstowych.
g) Musi mieć opcję okresowego przypominania o konieczności restartu telefonu.

Załącznik nr 2 do Umowy

…….....

Miejscowość, data

RAPORT - ROZLICZENIE CZASU WSPARCIA TECHNICZNEGO

Wzór

Na podstawie Umowy nr ……. zawartej w dniu …….. roku, informuję **o realizacji wsparcia technicznego, w okresie od dnia …….. do dnia ……**

Lp.	Zakres konsultacji	Data	Liczba minut
1.			
2.			
3.			

……

Wykonawca

OŚWIADCZENIE ZAMAWIAJĄCEGO

Potwierdzam przyjęcie /Odmawiam przyjęcia raportu z realizacji wsparcia technicznego *w zakresie dotyczącym wsparcia oznaczonego numerami ……. z uwagami poniżej**:

……

…….....

Miejscowość, data

……

Zamawiający

*niewłaściwe skreślić