Załącznik nr 4 do SWZ

Projektowane postanowienia umowy

Umowa nr ……..

zawarta w dniu…… **2024 roku w Krakowie** pomiędzy **Uniwersytetem Rolniczym in. Hugona Kołłątaja w Krakowie**,

z siedzibą pod adresem: 31-120 Kraków, al. Adama Mickiewicza 21, NIP: 675-000-21-18, REGON: 000001815, reprezentowanym przez:

…… ,

przy kontrasygnacie -…… ,

zwanym w treści umowy „Zamawiającym”,

a

…… z siedzibą …… wpisanym do …… pod numerem …… NIP: …… REGON: …… reprezentowanym przez: …… - ……

zwanym w treści umowy „Wykonawcą”,

łącznie zwanymi, również „Stronami”.

Umowa została zawarta na podstawie przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2023 r., poz. 1605 ze zm.) w wyniku rozstrzygnięcia postępowania o udzielenie zamówienia publicznego przeprowadzonego w trybie podstawowym na dostawy pn. Dostawa i wdrożenie oprogramowania klasy XDR dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie, któremu nadano numer referencyjny: DZiK -DZP.2921.41,2024.

§1

Definicje

EDR (Endpoint Detection and Response) umożliwia monitorowanie stacji końcowych pod kątem podejrzanego zachowania i rejestrować każdą aktywność czy zdarzenie. System następnie koreluje te informacje w celu wykrycia występowania zaawansowanych zagrożeń,

gdzie następnie uruchamia zautomatyzowane działania mające na celu zatrzymanie zagrożenia.

XDR (Extended Endpoint Detection and Response) to rozwinięcie systemu EDR. Podczas gdy EDR zbiera i koreluje dane z stacji końcowych, XDR rozszerza ten zakres poza stacje końcowe, zapewniając wykrywanie i analizę informacji także w sieciach, serwerach, chmurze, SIEM i wielu innych.

APT (Advanced Persistent Threats) - w ataku APT aktor wykorzystuje najbardziej wyrafinowane taktyki i technologie w celu penetracji sieci o wysokim profilu. Celem ataków APT jest pozostanie w ukryciu i eksploracja sieci, pozostając niewykrytym przez tygodnie, miesiące, a nawet lata.

AMSI (Antimalware Scan Interface) - to wbudowany w system Windows mechanizm do zaawansowanej ochrony przed złośliwym oprogramowaniem, używany między innymi do sprawdzania złośliwych skryptów.

Agent – to wszystkie aplikacje dostarczanego oprogramowania które muszą być zainstalowane na stacji końcowej.

Stacja robocza – komputery stacjonarne oraz laptopy

Stacja końcowa - dowolne urządzenie (stacja robocza / serwer / urządzenie mobilne) z dowolnym systemem operacyjnym wymienionym w Wymaganiach Ogólne (WO60) na którym jest zainstalowany agent oferowanego oprogramowania.

Systemy Microsoft Windows - rodzina systemów operacyjnych aktualnie wspieranych i stworzonych przez firmę Microsoft. Rodzina systemów operacyjnych działająca na serwerach oraz na stacjach roboczych.

MacOS - rodzina systemów operacyjnych aktualnie wspieranych i stworzonych przez firmę Apple Inc. Rodzina systemów operacyjnych działająca na stacjach roboczych.

Urządzenie mobilne - telefony komórkowe, smartfony, tablety wyposażone w system operacyjny iOS lub Android.

Konsola centralnego zarządzania – serwer lub serwery na których odbywa się zarządzanie wszystkimi agentami zainstalowanymi na stacjach końcowych.

§2

1. Przedmiotem niniejszej umowy jest dostawa i wdrożenie oprogramowania klasy XDR (Extended Endpoint Detection and Respose) dla Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie, zwanego dalej oprogramowaniem, zgodnie z niniejszą umową, złożoną ofertą na warunkach określonych w Specyfikacji Warunków Zamówienia.
2. Zaawansowane oprogramowanie chroniące stacje robocze, serwery i urządzenia mobilne które zapewni m.in.:
    1) funkcjonalność ochrony antywirusowej,
    2) aktywną ochronę stacji końcowych przed działaniem złośliwego oprogramowania i innych zaawansowanych cyberzagrożeń,
    3) możliwość gromadzenia informacji o zdarzeniach oraz rozubudowane funkcje reakcji na incydenty,
    4) detekcji zagrożeń, identyfikacji działań cyberprzestępców oraz zdarzeń z kategorii APT (Advanced Persistent Threats),
    5) aktywnej reakcji i odpowiedzi na wykryte zdarzenie oraz incydenty,
    6) realizacji działań proaktywnych w tym aktywnego wyszukiwania intruzów w infrastrukturze informatycznej.
3. Etapy realizacji zamówienia:

    ETPAP I Dostawa oprogramowani

    a) Wykonawca w terminie do 7 dni kalendarzowych od dnia podpisania Umowy zapewni Zamawiającemu możliwość pobierania zamówionego oprogramowania i kluczy licencyjnych za pośrednictwem witryny producenta - strony internetowej wskazanej przez Wykonawcę.
    b) Możliwość pobierania wersji instalacyjnych Oprogramowania producenta, o których mowa w lit. a) będzie zapewniona w trybie 24 godziny na dobę, 7 dni w tygodniu.

    ETPAPII Wdrożenie oprogramowania

    a) Wykonawca w terminie do 30 dni kalendarzowych od dnia podpisania Umowy wdroży wszystkie elementy oferowanego oprogramowania.
    b) Zamawiający w terminie 5 dni roboczych od dostarczenia przez Wykonawcę przygotowanego instalatora z agentem, zainstaluje go na co najmniej 100 stacjach końcowych.

c) Podstawą podpisania protokołu odbioru Etapu II będzie uruchomienie konsoli centralnego zarządzania i podpięcie do niej co najmniej 100 stacji końcowych.

ETAP III Dokumentacja powykonawcza i szkolenia

a) Wykonawca dostarczy dokumentację powykonawczą, przeprowadzi warsztaty oraz dostarczy vouchery na certyfikowane szkolenia producenta oferowanego oprogramowania nie później niż do 30 dni kalendarzowych od podpisania protokołu odbioru Etapu II.
b) Dokumentacja przekazana Zamawiającemu podlega weryfikacji w ciągu 5 dni roboczych, w przypadku wykrycia przez Zamawiającego błędów lub jeżeli dokumentacja będzie niepełna Wykonawca jest zobowiązany do poprawienia dokumentacji.
c) Wykonawca przekaże Zamawiającemu kompletną/poprawioną dokumentację przed podpisaniem protokołu odbioru końcowego.
d) Potwierdzeniem prawidłowej realizacji przedmiotu Umowy będzie podpisany protokół odbioru końcowego.

4. Wykonawca zobowiązuje się do wykonania przedmiotu umowy, o którym mowa w ust. 1, zgodnie ze szczegółowym Opisem Przedmiotu Zamówienia, stanowiącym Załącznik nr 1 do Umowy.
5. Wykonawca gwarantuje, iż licencja udzielona na oprogramowanie będące przedmiotem umowy, nie będzie wypowiedziana z przyczyn niezawinionych przez Zamawiającego. W przypadku wypowiedzenia licencji, wbrew zobowiązaniu o którym mowa powyżej, bez winy Zamawiającego, niezależnie od przyczyn takiego zdarzenia, włączając w to przyczyny, za które Wykonawca nie ponosi odpowiedzialności, Wykonawca zobowiązuje się do zapłaty na rzecz Zamawiającego 100% kwoty brutto należnej Wykonawcy, o której mowa w § 3 ust. 1 umowy.
6. Wykonawca oświadcza, iż przysługują mu odpowiednie prawa w zakresie umożliwiającym wykonanie umowy oraz, że jest uprawniony do udzielenia Zamawiającemu licencji do korzystania z oprogramowania na zasadach określonych w umowie.
7. Wykonawca gwarantuje, że oprogramowanie dostarczone Zamawiającemu jest wolne od wad prawnych.

8. W przypadku, gdy osoba trzecia wystąpi przeciwko Zamawiającemu z jakimkolwiek roszczeniem z tytułu korzystania z oprogramowania, które zostało dostarczone, Wykonawca zobowiązuje się do podjęcia na swój koszt i ryzyko kroków prawnych zapewniających należytą ochronę Zamawiającemu przed takimi roszczeniami. W szczególności Wykonawca zobowiązuje się zastąpić Zamawiającego, czy też w przypadku braku takiej możliwości, przystąpić po stronie Zamawiającego, do wszelkich postępowań toczących się przeciwko Zamawiającemu. Wykonawca zobowiązany będzie pokryć zasądzone koszty zastępstwa procesowego, koszty sądowe oraz zapłacić odszkodowania lub koszty polubownego załatwienia sprawy – w zakresie, w jakim Zamawiający uznał roszczenia osoby trzeciej.
9. Wykonawca zastrzega sobie prawo uczestniczenia w ewentualnym procesie lub negocjacjach osobiście lub poprzez ustanowionego pełnomocnika – w przypadku niedopuszczenia do udziału w procesie lub negocjacjach lub jednostronnego uznania przez Zamawiającego, Wykonawca nie ponosi odpowiedzialności z ust. 8.
10. Wykonawca dostarczy wraz z dokumentacją powykonawczą dokument gwarancyjny wystawiony przez producenta zaoferowanego oprogramowani, jeśli producent wystawia taki dokument.

§3

1. Za realizację przedmiotu umowy, Strony ustalają wynagrodzenie łączne **brutto** w wysokości **zł *(słownie: ……. …… złotych),*** w tym wynagrodzenie netto w wysokości ……. zł *(słownie:……. ……. złotych)*, należny podatek VAT w stawce …….% w wysokości …….. zł *(słownie: … złotych).*
2. W wynagrodzeniu, o którym mowa w ust. 1, ujęte są wszelkie koszty niezbędne do zrealizowania przedmiotu umowy, tj. koszty oprogramowania i wdrożenia, koszty przeprowadzenia szkoleń, koszty dokumentacji powykonawczej, koszty warsztatów, podatek VAT oraz wszelkie inne koszty, które nie zostały wymienione, ale są niezbędne do należytego wykonania przedmiotu umowy.
3. Wynagrodzenie, o którym mowa w ust. 1 obejmuje ryzyko Wykonawcy z tytułu oszacowania wszelkich kosztów związanych z realizacją przedmiotu Umowy, a także oddziaływania innych czynników mających wpływ na koszty.

4. Niedoszacowanie, pominięcie oraz brak rozpoznania zakresu przedmiotu Umowy nie może być podstawą do żądania zmiany wynagrodzenia określonego w ust. 1 niniejszego paragrafu.
5. Zamawiający umożliwia Wykonawcy zgodnie z zasadami określonymi w ustawie 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. z 2020 r., poz. 1666 ze zm.) przesyłanie ustrukturyzowanych faktur drogą elektroniczną. Zamawiający zobowiązany jest do odbierania od wykonawcy ustrukturyzowanych faktur elektronicznych za pośrednictwem Platformy Elektronicznego Fakturowania. Identyfikator Zamawiającego to numer NIP.
6. Zamawiający oświadcza, iż jest podatnikiem podatku VAT.
7. Za dzień zapłaty uznaje się dzień obciążenia rachunku Zamawiającego.

§4

1. Podstawą do wystawienia faktury stanowić będzie Protokół odbioru końcowego, o którym mowa w §2 ust. 3 ETAP III lit. d) niniejszej umowy.
2. Faktura za realizację przedmiotu umowy może zostać wystawiona najwcześniej w dniu podpisania Protokołu odbioru końcowego.
3. Zamawiający dokona płatności za realizację przedmiotu umowy na podstawie prawidłowo wystawionej faktury w terminie 30 dni od daty jej otrzymania, na rachunek Wykonawcy wskazany w fakturze.
4. Wykonawca wystawi Zamawiającemu fakturę na nabywcę - Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie, 31-120 Kraków, al. Mickiewicza 21, NIP: 675-000-21-18.
5. Faktura, oprócz wymaganych danych, powinna również zawierać numer umowy, z której realizacją wiąże się wypłata wynagrodzenia.
6. Zamawiający nie wyraża zgody na płatności częściowe.

§5

1. Wykonawca dostarczy i wdroży oprogramowanie, dokumentację powykonawczą i vouchery na certyfikowane szkolenie producenta oferowanego oprogramowania, a także przeprowadzi warsztaty, w terminie **do 60 dni kalendarzowych** licząc od daty zawarcia Umowy, z tym że:

Etap I – do 7 dni kalendarzowych od daty zawarcia umowy,

Etap II - do 30 dni kalendarzowych od daty zawarcia umowy,

Etap III – do 30 dni kalendarzowych od podpisania protokołu odbioru Etapu II.

2. Wykonawca dostarczy przedmiot niniejszej Umowy oraz przekaże wszystkie informacje konieczne do prawidłowego funkcjonowania oprogramowania na własny koszt do Centrum Informatyki Uniwersytetu Rolniczego im. Hugona Kołłątaja w Krakowie: al. Mickiewicza 21a, 31-120 Kraków.

§6

1. Wykonawca zobowiązuje się do zachowania w poufności wszystkich informacji dotyczących Zamawiającego oraz jego pracowników, współpracowników i podmiotów z Zamawiającym współpracujących, jakie Wykonawca uzyska w toku realizacji Umowy.
2. Wykonawca jest zwolniony z obowiązku zachowania tajemnicy i poufności materiałów i danych, o których mowa w ust. 1, jeżeli informacje, co, do których taki obowiązek istniał:
   1) w dniu ich ujawnienia były powszechnie znane bez zawinionego przyczynienia się wykonawcy do ich ujawnienia;
   2) muszą być ujawnione zgodnie z przepisami prawa, postanowieniami sądów lub właściwych organów państwowych;
   3) muszą być ujawnione w celu wykonania umowy, a wykonawca uzyskał zgodę zamawiającego na ich ujawnienie.
3. Wszelkie informacje o Zamawiającym uzyskane przez Wykonawcę w związku z realizacją przedmiotu Umowy mogą być wykorzystane tylko w celu wykonania Umowy.
4. Wykonawca odpowiada za podjęcie i zapewnienie wszelkich niezbędnych środków zapewniających dochowanie zasady poufności, określonej w ust. 1, przez swoich pracowników i podwykonawców.

§7

1. Wykonawca zapłaci Zamawiającemu kary umowne w następującej wysokości:
   1) za odstąpienie od Umowy z przyczyn leżących po stronie Wykonawcy lub wypowiedzenie Umowy z przyczyn leżących po stronie Wykonawcy – 10% wynagrodzenia brutto, o którym mowa w §3 ust. 1 niniejszej Umowy;
   2) za zwłokę w wykonaniu przedmiotu Umowy w terminie określonym w §5 ust. 1 Umowy z przyczyn leżących po stronie Wykonawcy – 0,005% wartości wynagrodzenia brutto, o którym mowa w §3 ust. 1 Umowy, za każdy dzień zwłoki w stosunku do wyznaczonego terminu;
   3) za każdy inny przypadek nienależytego wykonania umowy, rozumianego w szczególności jako naruszenie postanowień umowy – 0,05% wartości wynagrodzenia brutto, o którym mowa w §3 ust. 1 niniejszej Umowy;
2. Kary umowne mogą zostać potrącone z należności faktury. W przypadku braku możliwości potrącenia, kary umowne zostaną zapłacone w terminie 14 dni od dnia wezwania do zapłaty.
3. Zamawiający zachowuje prawo do odszkodowania uzupełniającego do wysokości poniesionej szkody na zasadach ogólnych.
4. Łączna, maksymalna wysokość kar umownych, których mogą dochodzić Strony wynosi 10% wartości brutto przedmiotu umowy, o której mowa w § 3 ust. 1 umowy.

§8

1. Zamawiający może odstąpić od umowy:
   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;
   2) jeżeli zachodzi co najmniej jedna z następujących okoliczności:
      a) dokonano zmiany umowy z naruszeniem art. 454 i art. 455 ustawy Pzp;

b) Wykonawca w chwili zawarcia umowy podlegał wykluczeniu na podstawie art. 108 ustawy Pzp;

c) 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;

d) w innych przypadkach przewidzianych umową lub powszechnie obowiązującymi przepisami prawa.

2. W przypadku, o którym mowa w ust. 1 pkt 2 lit. a), Zamawiający odstępuje od umowy w części, której zmiana dotyczy.

3. W przypadkach, o których mowa w ust. 1, Wykonawca może żądać wyłącznie wynagrodzenia należnego z tytułu udokumentowanego wykonania części umowy.

§9

Wykonawca nie może bez pisemnej zgody Zamawiającego dokonać cesji wierzytelności wynikających z niniejszej umowy lub przenieść obowiązek zapłaty kar umownych lub odszkodowań należnych Zamawiającemu.

§10

1. Zmiana istotnych postanowień niniejszej Umowy w stosunku do treści oferty, na podstawie, której dokonano wyboru Wykonawcy, jest dopuszczalna w szczególnie uzasadnionych przypadkach, na zasadach wskazanych w ust. 2 – 9.
2. Zmiana może obejmować:
   1) zmianę terminu realizacji przedmiotu zamówienia z powodu nieterminowego przekazania niezbędnych do jego realizacji informacji/danych przez Zamawiającego, o czas tego opóźnienia lub w przypadku wystąpienia w czasie realizacji umowy okoliczności uniemożliwiających terminowe wykonanie zobowiązań, tj. działanie siły wyższej. Pojęcie siły wyższej oznacza wszelkie wydarzenia, istniejące lub mogące

zaistnieć w przyszłości, które mają wpływ na realizację umowy, znajdujące się poza realną kontrolą stron i których nie można było przewidzieć lub, które choć przewidywalne były nieuniknione, nawet po powzięciu przez zamawiającego lub wykonawcę wszelkich uzasadnionych kroków dla uniknięcia takich wydarzeń. Pojęcie to obejmuje w szczególności takie wydarzenia jak: zamieszki, wojny, pożary, powodzie, huragany, trzęsienia ziemi, promieniowanie, epidemie, strajk generalny lub branżowy trwający dłużej niż 5 dni. Jeśli zamawiający lub wykonawca będzie stał w obliczu „siły wyższej" zobowiązany jest niezwłocznie poinformować druga stronę umowy o zaistniałej sytuacji, naturze problemu, przewidywanym czasie trwania oraz przewidywanych konsekwencjach, jak również podjąć działania w celu zminimalizowania możliwych szkód. Trudności finansowe zamawiającego lub wykonawcy nie mogą być traktowane, jako „siła wyższa".

3. Każda ze Stron przedkładając drugiej Stronie propozycję zmian spełniającą wymogi określone w ust. 2, wraz z tą propozycją przedłoży:
   1) opis proponowanych zmian i harmonogram wykonania zmian;
   2) propozycję dotyczącą jakichkolwiek koniecznych modyfikacji w terminach realizacji usługi/dostawy i szacunek, w jaki sposób zakładane zmiany wpłyną na termin realizacji przedmiotu umowy.
4. Po otrzymaniu propozycji, Wykonawca albo Zamawiający (w zależności od przypadku) w terminie 5 dni zatwierdzi bądź odrzuci otrzymaną propozycję zmiany bądź w tym terminie wystąpi do strony występującej z propozycją zmian przesyłając zmodyfikowaną propozycję zmian spełniającą wymogi opisane w ust. 2.
5. W przypadku upływu terminu podanego ust. 4 traktuje się, iż propozycja wprowadzenia zmian została odrzucona.
6. Do przesłanych zmodyfikowanych propozycji zmian mają zastosowanie postanowienia ust. 4 – 5.
7. W przypadku przyjęcia propozycji zmian wchodzą one w życie pod warunkiem objęcia ich pisemnym aneksem.
8. Każda zmiana do umowy wymaga formy pisemnej i musi być dokonana poprzez sporządzenie aneksu.

9. Zmiana umowy dokonana z naruszeniem postanowień ust. 1 – 8 jest nieważna.

§11*

1. Wykonawca zrealizuje niniejsze zamówienie własnymi siłami, bez udziału podwykonawców.
2. Wykonawca powierzy podwykonawcy (nazwa, adres) realizację niniejszego zamówienia w zakresie: …
3. Wykonawca odpowiada za działania lub zaniechania podwykonawców, jak za działania lub zaniechania własne.

§12

Inspektor Ochrony Danych Uniwersytetu Rolniczego w Krakowie realizuje swój obowiązek informowania kontrahentów pełniących rolę podmiotów przetwarzających o obowiązkach spoczywających na nich, wynikających z 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), wynikający z art. 39 ust. 1 litera a) tego rozporządzenia, poprzez swoją stronę internetową https:// iod.urk.edu.pl, na której umieścił stosowne informacje.

§13

1. Przedstawicielem Wykonawcy, upoważnionym do kontaktu w sprawach związanych z realizacją niniejszej Umowy jest Pani/Pan ……., e-mail: ……, tel. ……., fax. ……
2. Przedstawicielem Zamawiającego, upoważnionym do kontaktu w sprawach związanych z realizacją niniejszej Umowy jest Pani/Pan ……., e-mail: ……, tel. ……., fax. ……
3. Zmiana osób, o których mowa w ust. 1 i 2, nie stanowi zmiany umowy oraz nie wymaga sporządzenia aneksu, lecz pisemnej notyfikacji.

§14

1. Strony wskazują następujące adresy do doręczeń:
   1) Wykonawca - **……..**

2) Zamawiający – Uniwersytet Rolniczy im. Hugona Kołłątaja, Centrum Informatyki, ul. Czysta 21, 31-121 Kraków.

2. O każdej zmianie adresu, każda ze stron jest zobowiązana niezwłocznie powiadomić drugą stronę w formie pisemnej – pod rygorem uznania za skutecznie doręczoną korespondencje kierowaną listem poleconym na adres wymieniony w ust. 1.
3. Zmiana adresów, o których mowa w ust. 1, nie stanowi zmiany umowy oraz nie wymaga sporządzenia aneksu, lecz pisemnej notyfikacji.

§15

1. W sprawach nieuregulowanych niniejszą umową mają zastosowanie w szczególności przepisy Kodeksu cywilnego oraz ustawy Prawo zamówień publicznych.
2. Ewentualne spory wynikające z wykonania niniejszej umowy będą rozpatrywane przez sąd powszechny właściwy dla siedziby Zamawiającego według prawa polskiego.
3. Niniejsza umowa zostaje zawarta z dniem jej podpisania przez obie Strony umowy / Umowa zostaje zawarta z chwilą złożenia ostatniego z podpisów elektronicznych. **
   (w przypadku zawarcia umowy drogą elektroniczną)
4. Umowa została sporządzona w trzech jednobrzmiących egzemplarzach, z czego jeden otrzymuje Wykonawca, a dwa Zamawiający / Umowa została sporządzona zgodnie z art. 78^1 §1 ustawy z dnia 23 kwietnia 1964 r. ** *(w przypadku zawarcia umowy drogą elektroniczną)*

ZAMAWIAJĄCY **WYKONAWCA**

** zapis zostanie odpowiednio zmodyfikowany, zgodnie z ofertą Wykonawcy.*

*** w zależności od formy zawarcia umowy.*

Załącznik nr 1 do umowy

Wymagania dla dostarczonego oprogramowania – Etap I - „Dostawa Oprogramowania”

Wymagania ogólne	
WO1	Należy dostarczyć 3000 licencji na urządzenia wykorzystywane przez Zamawiającego. Rozwiązanie musi zapewnić możliwość używania oprogramowania na co najmniej: 2770 stacjach roboczych, 200 serwerach, 30 urządzeniach mobilnych.
WO2	Udzielone licencje zezwalać będą na swobodne przenoszenie oprogramowania pomiędzy tego samego typu stacjami końcowymi (pomiędzy stacjami roboczymi, pomiędzy serwerami oraz pomiędzy urządzeniami mobilnymi).
WO3	Udzielone licencje będą licencjami terminowymi obowiązującymi przez 3 lata, od daty podpisania protokołu odbioru etapu II, ale nie wcześniej niż od 20 czerwca 2024 r.
WO4	Licencja powinna umożliwiać działanie zakupionego oprogramowania na czas wdrożenia (tj. od dnia podpisania umowy do podpisania protokołu odbioru etapu II), aby Zamawiający nie pozostał bez ochrony stacji końcowych przy użyciu obecnie posiadanego oprogramowania lub oprogramowania zaoferowanego przez Wykonawcę. Czas ten nie wlicza się w czas ważności licencji określony w punkcie WO3.
WO5	Wykonawca zapewnia i zobowiązuje się, że korzystanie przez Zamawiającego z dostarczonego przedmiotu zamówienia nie będzie stanowić naruszenia majątkowych praw autorskich osób trzecich, w szczególności Zamawiającemu nie może być zaoferowane oprogramowanie, które jest zarejestrowane w bazach producentów jako przeznaczone do sprzedaży lub sprzedane do innego klienta końcowego.
WO6	Oferowane oprogramowanie w dniu składania ofert nie może być przeznaczony przez producenta do wycofania z produkcji lub ze sprzedaży.
WO7	Oferowane oprogramowanie musi umożliwiać zarządzanie stacjami końcowymi za pomocą mechanizmu konsoli centralnego zarządzania.
WO8	Wszystkie moduły oferowanego rozwiązania muszą pochodzić od jednego producenta w celu zapewnienia kompatybilności wszystkich elementów oraz prawidłowego funkcjonowania.
WO9	Oprogramowanie musi pochodzić bezpośrednio od producenta lub z oficjalnych i autoryzowanych przez producenta kanałów dystrybucyjnych w Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania.
WO10	Zamawiający wymaga aby wykonawca dostarczył najnowsze wersje oprogramowania i umożliwił jego aktualizacje w każdym momencie użytkowania objętym zakupioną licencją. Możliwość aktualizacji dotyczy zarówno konsoli

	centralnego zarządzania jak i agentów zainstalowanych na stacjach końcowych, oraz każdego innego składowego elementu nabywanego oprogramowania umożliwiającego jego poprawne funkcjonowanie.
WO11	Wykonawca dostarczy Zamawiającemu wszelkie dane niezbędne do prawidłowego uruchomienia i korzystania z Oprogramowania (np. klucze licencyjne, instalatory). W szczególności dokumentację przedwdrożeniową zawierającą pełną informację o wymaganiach sprzętowych oraz sieciowych niezbędnych do prawidłowego działania oferowanego oprogramowania. Jeśli zajdzie taka konieczność zamawiający będzie mógł zwracać się o nieodpłatne udzielenie takich informacji przez cały okres ważności licencji na dostarczane oprogramowanie.
WO12	Zamawiający oczekuje, że konsola centralnego zarządzania oprogramowaniem na stacjach końcowych zostanie zainstalowana na serwerach Zamawiającego lub jeżeli nie ma takiej możliwości będą to serwery producenta dostarczanego oprogramowania. Serwery muszą fizycznie znajdować się na terenie Unii Europejskiej. Przerwanie dostępu do konsoli centralnego zarządzania nie powoduje przerwania ochrony stacji końcowych.
WO13	W przypadku konsoli centralnego zarządzania zainstalowanej w na serwerach producenta, miesięczna dostępność konsoli centralnego zarządzania musi wynosić nie mniej niż 99,5%.
WO14	W przypadku instalacji na serwerach Zamawiającego rozwiązanie musi dawać możliwość instalacji zarówno na serwerze fizycznym jak i w postaci maszyny wirtualnej. Rozwiązanie musi wspierać co najmniej następujące środowiska wirtualizacji Microsoft Hyper-V, Vmware.
WO15	Zamawiający wymaga aby komunikacja agenta zainstalowanego na stacjach końcowych z serwerami producenta oraz z konsolą centralnego zarządzania odbywała się szyfrowanym protokołem, a wszystkie dane zebrane były przechowywane i przetwarzane na obszarze Unii Europejskiej.
WO16	Oferowane rozwiązanie musiało być poddane ewaluacji przez MITRE ENGENUITY, ATT&CK Evaluations i musiało być oceniane przynajmniej w dwóch z trzech ewaluacji: • Turla (2023 r.) • Wizard Spider + Sandworm (2022 r.) • Carbanak+FIN7 (2021 r.)
WO17	Oferowane rozwiązanie musiało brać udział w teście skuteczności ewaluacji MITRE ENGENUITY, ATT&CK w ewaluacji Turla (2023) i uzyskać mniej niż 25 % braku wykryć (none detections) oraz brak udziału (Not applicable) w scenariusz Carbon i Snake (co oznacza relatywnie niską wykrywalność etapów ataku „substeps”) W scenariuszu Carbon istnieje 76 etapów ataku (substeps), w scenariuszu Snake istnieje 67 etapów ataku, łącznie 143 etapy ataku (substeps). M – liczba procent nie wykrytych etapów ataku Le – maksymalna liczba wszystkich etapów ataku (substeps)

	Lb – suma etapów ataku (substeps) 'None' i 'Not applicable' badanej oferty M = Lb / Le * 100%
WO18	Producent oferowanego systemu posiada certyfikat ISO 27001 lub SOC 2 type 2.
WO19	Dostarczone oprogramowanie musi posiadać interfejs w języku polskim lub angielskim.
WO20	Dostęp do konsoli centralnego zarządzania z poziomu interfejsu WWW zabezpieczonego za pomocą aktualnie zalecanego protokołu SSL/TLS (HTTPS).
WO21	Konsola centralnego zarządzania musi być wspierana przez następujące przeglądarki: Microsoft Edge, Mozilla Firefox, Google Chrome, w wersji aktualnej na dzień podpisania umowy.
WO22	Dostarczone oprogramowanie musi posiadać dwustopniowa autoryzację podczas logowania do konsoli centralnego zarządzania (dotyczy co najmniej konsoli centralnego zarządzania znajdującej się w na serwerach producenta).
WO23	Dostarczone oprogramowanie musi posiadać możliwość zakładania lokalnych kont użytkowników oraz definiowania ról i zestawów uprawnień dla tych użytkowników.
WO24	Dostarczone oprogramowanie musi posiadać możliwość tworzenia grup stacji końcowych.
WO25	Rozwiązanie ma możliwość definiowania różnych profili ustawień dla stacji końcowych z poziomu konsoli centralnego zarządzania. Profile te mogą być przypisane do pojedynczych stacji końcowych lub do grup.
WO26	Dostarczone oprogramowanie musi posiadać możliwość konfiguracji i monitorowania wszystkich modułów dostarczonego rozwiązania zainstalowanych na stacjach końcowych, ich aktualizację oraz zlecanie im zadań z poziomu konsoli centralnego zarządzania.
WO27	Konsola centralnego zarządzania musi umożliwiać wgląd w szczegóły zgłaszającego się hosta, w których zawarte są co najmniej informacje dotyczące: • kto jest zalogowany na stacji roboczej • systemu operacyjnego • wersji systemu operacyjnego • stanu zaszyfrowania dysków systemowych • adresów IP • wersji zainstalowanego oferowanego przez Wykonawcę produktu • wersji programu i bazy wirusów • ostatniej aktualizacji • stanu ochrony • aktualnych ustawień programu • przypisanej polityki (konfiguracji) • wyników skanowania skanera na żądanie • akcji związanych z wykrytymi zagrożeniami i skanowaniami
WO28	Konsola centralnego zarządzania musi umożliwiać filtrowania po różnych parametrach stacji końcowej z zainstalowanym agentem. Filtry muszą uwzględniać co najmniej:

	• system operacyjny • adres IP • nazwę stacji końcowej • które stacje końcowe były online w ciągu ostatnich 24 godzin, 7 lub 30 dni
WO29	Konsola centralnego zarządzania ma możliwość definiowania wykluczeń m.in. w zakresie: • ochrony antywirusowej w czasie rzeczywistym • skanowania na żądanie • ochrony behawioralnej
WO30	Konsola centralnego zarządzania umożliwia wysyłanie minimum następujących zadań do agenta zainstalowanego na stacji końcowej: • skanowanie komputera • izolacji komputera, usunięcia komputera z izolacji • zebrania logów z klienta • zaszyfrowania dysków systemowych • odinstalowania agenta
WO31	Dostarczone rozwiązanie posiada funkcjonalność generowania raportów, w tym w formie graficznej z poziomu konsoli centralnego zarządzania. Raporty mogą być generowane ręcznie lub automatycznie (według ustalonego harmonogramu)
WO32	Dostarczone rozwiązanie pozwala na eksport raportów w postaci plików PDF.
WO33	Dostarczone rozwiązanie posiada możliwość stworzenia archiwum zawierającego dodatkowe informacje dotyczące stacji końcowej, na której wystąpiła detekcja w celu przeprowadzenia analizy śledczej incydentu.
WO34	Dostarczone rozwiązanie pozwala na raportowanie u ilu użytkowników wykryto podejrzane działania oraz jakie jest ich nasilenie, tworzenie raportów zawierających co najmniej listę wygenerowanych detekcji, wraz z ich opisem, za zadany okres.
WO35	Raporty z wykrytych infekcji zawierają minimum: • informacje na temat źródła ataku • pliki jakie zostały zaatakowane przez wirusa • adresy sieciowe do jakich niebezpieczny proces próbował się połączyć • informacje na temat wyleczenia lub usunięcia wirusa • mapowanie wykrytych metod ataku na matrycę MITRE ATT&CK
WO36	Dostarczone rozwiązanie pozwala na automatyczne powiadamianie o pojawiających się zagrożeniach wraz z określeniem czy stacja końcowa jest odpowiednio zabezpieczona.
WO37	Dostarczone rozwiązanie pozwala na zarządzanie powiadomieniami.
WO38	Dostarczone rozwiązanie posiada możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. Co najmniej dla stacji końcowych z systemami Microsoft Windows wykluczenia muszą dotyczyć procesu lub procesu „rodzica”.
WO39	Dostarczone rozwiązanie pozwala na powiadomienia w przypadku, gdy podsystemy bezpieczeństwa agenta nie będą funkcjonowały poprawnie.

WO40	Dostarczone rozwiązanie pozwala na wysyłanie powiadomień poprzez e-mail.
WO41	Dostarczone rozwiązanie posiada "Dashboard" (konsolę) prezentujący incydenty w czasie rzeczywistym oraz ma możliwość definiowanie własnych "Dashboardów" z wykorzystaniem predefiniowanych "Widgetów" (kontrolek).
WO42	Dostarczone rozwiązanie posiada interaktywny interfejs użytkownika, tzn. że po wybraniu interesującego elementu, następuje przekierowanie do zawierającego bardziej szczegółowe.
WO43	Dostarczone rozwiązanie posiada podgląd wykrytych zagrożeń umożliwiający odfiltrowania ich według: • daty • kategorii • typu zagrożenia • działań naprawczych • poziomu ryzyka
WO44	Interfejs użytkownika tworzy widok incydentu zawierający kluczowe informacje, takie jak: • przyczyna źródłowa • lista urządzeń na których zarejestrowano podejrzane zdarzenia • zakres ataku (powiązane maszyny i konta użytkowników) • data i czas wystąpienia podejrzanych zdarzeń • listę podejrzanych zdarzeń zidentyfikowanych przez rozwiązanie • wykonanie wiersza poleceń używane do uruchomienia procesu • opis dla każdego z podejrzanych zdarzeń, wyjaśniający, dlaczego dane zdarzenie zostało uznane za podejrzane • sumę kontrolną plików, które zostały uznane za podejrzane • poszczególne fazy ataku zaprezentowane na osi czasu • komunikacja sieciowa nawiązana w trakcie trwania ataku • poziom ryzyka, określający istotność danej detekcji • typ detekcji, określający techniki ataku, które zostały wykryte podczas tworzenia detekcji (np. nieuprawnione podniesienie uprawnień, połączenia z sieciami C&C, nieuprawnione wykonanie skryptu) • zdarzenia które wskazują na wykorzystanie znanej techniki ataku na systemy informatyczne, zawierają odnośniki do ogólnodostępnych materiałów opisujących zastosowanie tych technik (np. matryca MITRE ATT&CK) • zdarzenia, występujące w detekcjach, które odnoszą się do plików oraz aplikacji uruchomionych na monitorowanych komputerach, zawierają odnośniki do ogólnodostępnej bazy reputacji, pozwalającej sprawdzić reputację tych plików (np. VirusTotal)
WO45	Dostarczone rozwiązanie posiada mechanizm pozwalający na wyszukiwanie i ”polowanie” na zagrożenia sieciowe. Mechanizm ten posiada różne znaczniki, z których można budować zapytania.
WO46	Dostarczone rozwiązanie umożliwia wyszukanie zdarzeń napływających do konsoli co najmniej w oparciu o: • PID nowego procesu

	• ścieżkę • nazwę procesu docelowego • nazwa pliku • typ zdarzenia • nazwę systemu • typ systemu • adres IP źródłowy • adres IP zdalny • port lokalny • port zdalny • adres URL • wartość klucza rejestru
WO47	Dostarczone rozwiązanie umożliwia przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem zapytań.
WO48	Dostarczone rozwiązanie zapewnia predefiniowane zapytania dotyczące artefaktów kryminalistycznych (np. hash, domena, nieprzetworzone zdarzenia, klucze rejestru). Reguły tworzenia zapytań muszą być opisane w dokumentacji systemu.
WO49	Dostarczone rozwiązanie posiada możliwość szybkiego podglądu otwartych incydentów, najczęstszych powiadomień, urządzeń które mają najczęściej problem oraz możliwość wyświetlenia zablokowanych hashy plików.
WO50	Dostarczone rozwiązanie na bazie zebranych danych w czasie rzeczywistym generuje detekcje, które stanowią powiązane ze sobą podejrzane zdarzenia, zebrane przez agentów ze stacji końcowych.
WO51	Dostarczone rozwiązanie koreluje alerty, incydenty, zdarzenia wykryte w ramach wykrytego ataku, mapuje na matrycę taktyk, technik i procedur w ramach frameworku (metodyki) MITRE ATT&CK.
WO52	Dostarczone rozwiązanie automatyczne koreluje powiązane alerty wykryte na różnych stacjach końcowych w celu przyspieszenia i ułatwienia klasyfikacji oraz analizy incydentu. Wygenerowany skonsolidowany incydent prezentuje graficzną oś czasu, na której umieszczone będą kluczowe zdarzenia i podejrzenia, uruchamiane procesy, rozprzestrzenianie się ataku na kolejne stacje, wraz z możliwością interaktywnego śledzenia szczegółów tych zdarzeń.
WO53	Dostarczone rozwiązanie pokazuje kompletny widok drzewa ataku dla każdego złośliwego i niezłośliwego procesu zawierającego szczegółowe informacje dotyczące poszczególnych elementów biorących udział w wykrytej anomalii. Automatycznie dostarcza informacji o urządzeniach i kontach użytkowników, które zostały dotknięte lub brały udział w przebiegu ataku. Detekcje widoczne są w konsoli zarządzającej w postaci graficznych diagramów.
WO54	Dostarczone rozwiązanie pozwala na dodawanie komentarzy do incydentów, w celu łatwiejszego ich procesowania i przekazywania pomiędzy analitykami. System pozwala na przypisywanie zdarzeń/incydentów operatorom systemu.

WO55	Dostarczone rozwiązanie umożliwia oznaczanie wygenerowanych detekcji jako błędnej.
WO56	Dostarczone rozwiązanie posiada wbudowane reguły, po których wystąpieniu, nastąpi wyzwolenie alarmu bezpieczeństwa. Istnieje możliwość utworzenia własnych reguł.
WO57	Dostarczone rozwiązanie posiada możliwość wprowadzania wykluczeń, po których nie zostanie wyzwolony alarm bezpieczeństwa. wykluczenia muszą dotyczyć procesu lub procesu „rodzica”. Kryteria wykluczeń są konfigurowane w oparciu o przynajmniej: • nazwę procesu • ścieżkę procesu • hash pliku
WO58	Dostarczone rozwiązanie posiada możliwość eksportu logów audytowych poprzez Syslog po SSL/TLS w formacie CEF.
WO59	Dostarczone rozwiązanie posiada interfejs API do integracji z popularnymi narzędziami do orkiestracji i automatyzacji.
WO60	Na dzień podpisania umowy oprogramowanie musi wspierać ochronę stacji końcowych z poniższymi systemami operacyjnymi : Microsoft Windows 7, Microsoft Windows 10, Microsoft Windows 11, MacOS Sonoma 14.x, MacOS Ventura 13.x, MacOS Monterey 12x, Microsoft Windows Server 2016, Microsoft Windows Server 2019, Microsoft Windows Server 2022, Ubuntu (20.04, 22.04), Debian (10-12), RHEL (8-9), CentOS (7-9), Amazon Linux (2, 2023), SUSE (15), Android (10-14), iOS 15, iOS 16.
WO61	Dostarczone rozwiązanie musi umożliwiać instalację agenta zarówno na fizycznych maszynach jak i w środowisku wirtualnym.
WO62	Dostarczone rozwiązanie musi wspierać następujące metody instalacji agenta na stacjach końcowych: • instalacja z wykorzystaniem mechanizmów dystrybucji oprogramowania Active Directory • ręcznej instalacji
WO63	Dostarczone rozwiązanie zapewnia nieprzerwane działanie agenta i ochronę stacji końcowej od momentu startu systemu operacyjnego aż do momentu zamknięcia systemu operacyjnego.
WO64	Dostarczone rozwiązanie zapewnia aktualizację agenta zainstalowanego na stacji końcowej do nowej wersji, następuje ona w sposób automatyczny, niewidoczny dla użytkownika końcowego. Wszystkie aktualizacje definicji wirusów lub bazy sygnatur nie wymagają restartu systemu operacyjnego.
WO65	Dostarczone rozwiązanie zapewnia możliwość ręcznej aktualizacji agenta lub definicji wirusów.
WO66	Dostarczone rozwiązanie musi umożliwić zabezpieczenia agenta przed deinstalacją przez niepowołaną osobę, nawet gdy posiada ona prawa lokalnego

	lub domenowego administratora, przy próbie deinstalacji program będzie pytał o hasło.
WO67	Dostarczone rozwiązanie zapewnia komunikację agenta zainstalowanego na stacjach końcowych z konsolą centralnego zarządzania z interwałem nie dłuższym niż 10 min.
WO68	Dostarczone rozwiązanie zapewnia ochronę stacji końcowych w trybie offline.
WO69	Dostarczone rozwiązanie zapewnia po stronie stacji końcowej mechanizm buforowania danych w przypadku braku połączenia z konsolą centralnego zarządzania (np. praca w trybie offline). Dane zebrane na stacji końcowej są przesłane do analizy od razu po uzyskaniu przez agenta dostępu do sieci Internet.
WO70	Stacje końcowe nie nawiązujące komunikacji z konsolą zarządzającą mogą być automatycznie usuwane z listy po określonym przez administratora czasie.
WO71	Agent zainstalowany na stacjach końcowych posiada możliwość zarejestrowania się w Windows Security Centre jako pełnoprawne rozwiązanie antywirusowe.

Wymagania dotyczące ochrony (co najmniej stacji roboczych i serwerów z systemami Microsoft Windows)	
WS1	Dostarczone rozwiązanie posiada mechanizm ochrony w czasie rzeczywistym opartym na bazie definicji wirusów dla stacji końcowych z systemami Microsoft Windows, MacOS, Linux.
WS2	Dostarczone rozwiązanie posiada mechanizm Antymalware dla stacji końcowych z systemami Microsoft Windows, MacOS, Linux.
WS3	Dostarczone rozwiązanie umożliwia skanowanie plików niewykonywalnych (dokumentów, ogólnych formatów plików) w systemach Microsoft Windows, MacOS, Linux.
WS4	Dostarczone rozwiązanie posiada funkcjonalność ochrony UEFI.
WS5	Dostarczone rozwiązanie posiada mechanizm wykrywania i przeciwdziałania nowym i nieznanym zagrożeniom, bazujący na: • modelu uczenia maszynowego (ang. Machine Learning - ML) • analizie behawioralnej, która wykrywa wzorce zachowań atakującego • algorytmach wykrywania anomalii oraz profilowania komputera i jego użytkownika • wykrywaniu anomalii w ruchu sieciowym • technologii chmurowej • technologii heurystycznej
WS6	Dostarczone rozwiązanie posiada następujące funkcjonalności w zakresie ochrony przed ransomware: • wykrywanie ataków ransomware, w szczególności tych których celem jest uszkodzenie Master Boot Record (MBR) niezależnie od tego, czy zostały uruchomione lokalnie, czy ze zdalnego punktu końcowego • w przypadku wykrycia ataku przerwanie próby szyfrowania plików na dysku oraz dodanie procesu odpowiedzialnego za szyfrowanie do listy procesów, których nie będzie można ponownie uruchomić na innych stacjach końcowych
WS7	Dostarczone rozwiązanie wspiera technologię Antimalware Scan Interface (AMSI) w celu odbierania i analizowania zdekodowanych skryptów.
WS8	Dostarczone rozwiązanie posiada mechanizm ochrony przed zagrożeniami uruchamianymi z dysków zmapowanych, pamięci przenośnych, przed zagrożeniami płynącymi z plików odebranych przez klienta poczty elektronicznej, zagrożeń pobranych przez przeglądarkę internetową oraz wynikających z innych połączeń sieciowych.
WS9	Dostarczone rozwiązanie zapewnia ochronę przed atakami wykorzystującymi legalne narzędzia systemowe w podejrzany sposób poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie taktyk, technik i procedur stosowanych przez cyberprzestępców.
WS10	Dostarczone rozwiązanie jest w stanie wykryć fazę "ruchu bocznego" ataku - ang. Lateral Movement (np. ataki Pass-the-hash, zdalne tworzenie zaplanowanego zadania itp.).

WS11	Dostarczone rozwiązanie wykrywa i zapobiega atakom bezplikowym, działającym tylko w pamięci operacyjnej.
WS12	Dostarczone rozwiązanie zapewnia ochronę przed wykorzystywaniem exploitów w pamięci Windows (np. exploity 0-day), w tym: Mandatory ASLR, DEP.
WS13	Dostarczone rozwiązanie zapewnia ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu poprzez wykrywanie prób wykorzystania co najmniej następujących technik eksploitacji: Kernel Privilege Escalation, ROP.
WS14	Dostarczone rozwiązanie posiada mechanizmy prewencji, które będą blokowały wykonanie złośliwej aktywności w trybie przed wykonaniem (ang. pre-execution), a także przerwanie złośliwej aktywności w trakcie wykonania (ang. on-execution). W ramach działania silników prewencyjnych systemu jest dostępna opcja automatycznego przeniesienia do kwarantanny plików uznanych za niebezpieczne.
WS15	Dostarczone rozwiązanie ma możliwość odizolowania stacji końcowej od sieci, jednocześnie zapewniając ciągłość analizy przeprowadzanej na tej stacji końcowej dla operatora systemu. Dostarczone rozwiązanie ma możliwość cofnięcia izolacji sieciowej maszyny z konsoli centralnego zarządzania.
WS16	Dostarczone rozwiązanie ma możliwość zestawienia sesji Remote Shell do wybranych stacji, udostępniając operatorowi linię poleceń systemu operacyjnego (np. PowerShell dla systemu Windows). Dostarczone rozwiązanie przechowuje pełny log z wykorzystania funkcji Remote Shell, w którym zachowane będą wszystkie komendy wydawane podczas nawiązanej sesji ze stacją końcową.
WS17	Dostarczone rozwiązanie pozwala na wykonanie akcji naprawczych na stacji końcowej. Dostarczone rozwiązanie dostarcza automatycznie zestaw działań naprawczych, jakie należy wykonać w przypadku danego typu wykrytego zagrożenia.
WS18	Dostarczone rozwiązanie w ramach odpowiedzi na incydent umożliwia: • reakcje (remediację) ze wskazaniem kroków, które mogą być podjęte automatycznie • uruchomienie skryptu na stacji końcowej • nawiązanie interaktywnego połączenia do linii poleceń na stacji końcowej • wyłączenie procesu na stacji końcowej • izolację sieciową stacji końcowej • usunięcie pliku na stacji końcowej • przeniesienie pliku na stacji końcowej do kwarantanny
WS19	Dostarczone rozwiązanie posiada funkcjonalność analizatora w środowisku sandbox.
WS20	Dostarczone rozwiązanie umożliwia: • skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików • skanowanie całego dysku, wybranych katalogów lub pojedynczych plików „na żądanie”

	• skanowanie podmontowanych dysków sieciowych • skanowanie urządzeń przenośnych takich jak pendrive, dyski zewnętrzne itp. Skanowanie to może odbywać się w sposób automatyczny bez wiedzy użytkownika
WS21	Dostarczone rozwiązanie umożliwia umieszczenia na liście wykluczeń ze skanowania wybranych katalogów lub plików na podstawie: • rozszerzenia • sumy kontrolnej • lokalizacji pliku
WS22	Dostarczone rozwiązanie posiada następujące funkcjonalności w zakresie kontroli urządzeń zewnętrznych: • mechanizm kontroli urządzeń zewnętrznych (urządzania USB, pamięci masowe, napędy CD/DVD, modemy, porty LPT/COM, drukarki, czytniki kart pamięci, kamery, urządzenia bluetooth) • możliwość tworzenie reguł dla podłączanych urządzeń w oparciu o numer seryjny • możliwość blokady zapisywania plików na zewnętrznych dyskach USB, urządzenia takie są wówczas dostępne w trybie tylko do odczytu • możliwość zdefiniowanie listy zaufanych urządzeń, które nie będą blokowane podczas podłączania do stacji końcowej
WS23	Dostarczone rozwiązanie posiada funkcjonalność zapory sieciowe lub możliwość wykorzystania natywnych narzędzi wbudowanych w system.
WS24	Dostarczone rozwiązanie posiada funkcjonalność pełnego szyfrowania dysku lub możliwość wykorzystania natywnego szyfrowania wbudowanego w systemy Microsoft Windows i MacOS.
WS25	Dostarczone rozwiązanie zbiera całą telemetrię aktywnie w czasie zbliżonym do rzeczywistego (bez wymaganej interakcji użytkownika dla wszystkich typów danych).
WS26	Telemetria ze stacji końcowych objętych ochroną jest przechowywana centralnie, aby móc korelować zdarzenia między różnymi stacjami.
WS27	Wszystkie procesy związane z analizą zebranych danych oraz wykrywaniem podejrzanych zdarzeń odbywa się na serwerze, a nie na monitorowanej stacji końcowej.
WS28	Dostarczone rozwiązanie zapewnia ochronę na podstawie zachowań opisywanych przez dane telemetryczne zbierane ze stacji końcowych.
WS29	Dostarczone rozwiązanie dokonuje analizy danych telemetrycznych ze stacji końcowych bez jakiegokolwiek filtrowania tych danych po stronie stacji końcowej.
WS30	Dostarczone rozwiązanie nie ogranicza liczby zdarzeń danego typu (np. limitowana liczba zapytań DNS w określonym przedziale czasowym, itp.).
WS31	Telemetria zbierana ze stacji końcowych uwzględnia minimalnie takie elementy jak: • połączenia sieciowe do/ze stacji, w tym takie szczegóły jak: ○ adresy

	○ porty ○ stan połączenia ○ ilość danych otrzymanych/wysłanych ○ czas utworzenia połączenia • działania na plikach, operacje: ○ utworzenia ○ zmiany nazwy ○ usunięcia pliku ○ zapisywanie ○ przesunięcie ○ modyfikacja ○ wraz z informacją o tym, jaki proces wykonywał dane działanie oraz jaki użytkownik jest zalogowany w systemie podczas tej operacji • operacje w rejestrze ○ skasowanie wartości ○ ustawienie wartości ○ utworzenie klucza ○ kasowanie klucza ○ zmiana nazwy klucza • utworzenie nowego procesu i zakończenie procesu
WS32	Dostarczone rozwiązanie musi być dostarczone z funkcją umożliwiającą przetwarzanie i przechowywanie danych telemetrycznych z następujących systemów: • stacje końcowe • zdarzenia/logi (ang. events) z Active Directory i Azure Entra ID (Azure Active Directory) lub ochrania aplikacje Microsoft Office 365 i Google Workspace. Jeśli funkcjonalność wymaga dodatkowych licencji, licencje powinny zostać dostarczone wraz z oferowanym oprogramowaniem.
WS33	System przechowuje szczegółowe dane telemetryczne z wszystkich zabezpieczonych agentem stacji końcowych przez co najmniej 30 dni.
WS34	System przechowuje informacje o alarmach minimum przez okres 180 dni.
WS35	System przechowuje informacje o incydentach minimum przez okres 180 dni.

Wymagania dla dostarczonego oprogramowania – Etap II – „Wdrożenie oprogramowania”

Wymagania dotyczące wdrożenia	
WW1	Zamawiający wymaga aby Wykonawca przydzielił do wdrożenia zaoferowanego rozwiązania co najmniej 2 osoby posiadające aktualny certyfikat (dotyczący znajomości i obsługi) wystawiony przez producenta wdrażanego oprogramowania oraz osoby przydzielone posiadały minimum 2 lata doświadczenia we wdrażaniu oferowanego rozwiązania.
WW2	Zakres wdrożenia musi obejmować wszystkie elementy oferowanego systemu.
WW3	Zamawiający dopuszcza wdrożenie i konfigurację oferowanego systemu w formie zdalnej.
WW4	Konfiguracja oferowanego systemu zostanie wykonana przez Wykonawcę w uzgodnieniu z Zamawiającym.
WW5	Prace będą wykonywane przy asyście i obecności oddelegowanego pracownika Zamawiającego.
WW6	Instalacja lub uruchomienie konsoli centralnego zarządzania w zależności od rozwiązania oferowanego przez Wykonawcę.
WW7	Dodanie min. 2 głównych administratorów, min. 2 użytkowników systemu do konsoli centralnego zarządzania.
WW8	Przygotowanie min. 2 zestawów uprawnień dla różnych grup użytkowników systemu w konsoli centralnego zarządzania.
WW9	Przygotowanie profili konfiguracyjnych w zależności od typu stacji końcowej z ustawieniami dla agentów.
WW10	Przygotowanie instalatorów z agentem do wdrożenia na stacjach końcowych.
WW11	Zamawiający wdroży/zainstaluje na stacjach końcowych agentów we własnym zakresie.
WW12	Konfiguracja powiadomień i integracja z systemem pocztowym Zamawiającego.
WW13	Przygotowanie przykładowych raportów w konsoli centralnego zarządzania.
WW14	Wykonanie testów poprawności działania całego systemu w szczególności sprawdzenie czy oferowany system poprawnie reaguje na zagrożenia.

Wymagania dla dostarczonego oprogramowania – Etap III – „Dokumentacja powykonawcza i Szkolenia”

Zamawiający wymaga od Wykonawcy dostarczenia dokumentacji powykonawczej. Dokumenty powinny być dostarczone w formie elektronicznej.

Wymagania dotyczące dokumentacji powykonawczej	
DP1	Opis wdrożonego systemu wraz z szczegółowym opisem jego poszczególnych modułów oraz schematami funkcjonalnymi.
DP2	Opis instalacji i konfiguracji systemu, w tym zmiennych środowiskowych.
DP3	Konfigurację systemu.
DP4	Zestawienie adresacji, protokołów i portów IP oraz danych dostępowych utworzonych użytkowników.
DP5	Konfiguracja profili stacji końcowych.
DP6	Opis procedur utrzymaniowych i administracyjnych w szczególności aktualizacji poszczególnych modułów systemu.
DP7	Opis procedury wykonywania kopii zapasowej oraz archiwizacji systemu.
DP8	Opis procedur awaryjnych oraz „disaster recovery”.
DP9	Dokumentacja musi zostać przygotowana w języku polskim.

Wymagania dotyczące warsztatów organizowanych przez Wykonawcę	
SW1	Wykonawca zobowiązany jest przeprowadzić warsztaty dla maksymalnie 15 osób wskazanych przez Zamawiającego.
SW2	Zamawiający zastrzega sobie prawo do możliwości utrwalenia wszelkich materiałów szkoleniowych oraz przebiegu warsztatów w postaci materiału wideo do późniejszego wielokrotnego odtwarzania przez Zamawiającego i tylko na użytek wewnętrzny Zamawiającego.
SW3	Warsztaty będą omawiały wszystkie komponenty dostarczonego oprogramowania.
SW4	Językiem warsztatów musi być język polski.
SW5	Wykonawca zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej w języku polskim.
SW6	Czas warsztatów: nie mniej niż 3 dni (czas całego warsztatu nie mniej niż 18 godzin, warsztaty w godzinach pracy Zamawiającego od 8:00 do 16:00). Jeżeli Wykonawca uważa, że jest potrzebny dłuższy okres na przekazanie omawianego zakresu materiału, Zamawiający dopuszcza dłuższy czas warsztatów.
SW7	Warsztaty odbędą się w kilku grupach (grupa 4-6 osób). O przypisaniu użytkownika do grupy oraz ilości użytkowników w poszczególnych grupach decyduje Zamawiający. Zakres warsztatów będzie ustalany z Zamawiającym, który moduł szkolenia powinien być bardziej lub mniej rozwinięty w zależności do której grupy jest kierowany.
SW8	Warsztaty mogą odbyć się w formie zdalnej.
SW9	Wykonawca przygotuje na potrzeby przeprowadzenia warsztatów wszelkie niezbędne zaplecze techniczne tj. środowiska informatyczne dla poszczególnych uczestników, wirtualną salę laboratoryjną, oprogramowanie, licencje. Każdy uczestnik warsztatów będzie miał przydzielone własne środowisko informatyczne.
SW10	Osoba prowadząca warsztaty powinna posiadać aktualny certyfikat (dotyczący znajomości i obsługi) wystawiony przez producenta wdrażanego oprogramowania oraz minimum 2 lata doświadczenia we wdrażaniu oferowanego rozwiązania.
SW11	Po zakończeniu warsztatów Wykonawca przekaże uczestnikom certyfikaty uczestnictwa.
SW12	Wykonawca przeprowadzi instruktaż omawiający wszystkie elementy składowe dostarczanego rozwiązania, który będzie dotyczył konfiguracji oraz administracji dla pracowników Zamawiającego. Zakres warsztatów zostanie ustalony z Wykonawcą po wyborze najlepszego rozwiązania. Zakres powinien odnosić się bezpośrednio do przedmiotowego wdrożenia i obejmować co najmniej: • omówienie wszystkich komponentów systemu • wdrożenie systemu • utrzymanie systemu • zarządzanie oferowanym systemem • konfiguracja powiadomień i raportów

	• obsługa konsoli centralnego zarządzania • tworzenie dostępu do konsoli centralnego zarządzania • zarządzanie uprawnieniami • tworzenie pakietów instalacyjnych agentów • wdrożenie ręczne oraz zdalne agentów • profile / polityki bezpieczeństwa agentów • omówienie opcji występujących w politykach, zwróceniem uwagi na najważniejsze ustawienia pod kątem stacji końcowych • zarządzanie grupami chronionych urządzeń końcowych • przypisywanie reguł do grup lub urządzeń końcowych • zarządzanie agentami chronionych urządzeń końcowych • rozwiązywanie problemów z agentem • rozwiązywanie podstawowych problemów przy administracji • tworzenie reguł bezpieczeństwa i wyjątków od nich • ochronę przed malware • ochronę przed exploit • obsługę wykrytych incydentów • podstawowe i zaawansowane odpowiedzi na ataki • konfiguracja zapory sieciowej • obsługa i zarzadzanie szyfrowaniem stacji roboczych i serwerów • obsługa systemu XDR • Threat Hunting • sposób wykorzystywania zebranych danych • jak tworzyć zapytania na potrzeby wyszukiwania kluczowych elementów zdarzeń • głęboka analiza incydentów z uwzględnieniem artefaktów (np. IP, Hash) • wykrywanie zagrożenia APT • wykonywanie analizy po włamaniowej • zagadnienia związane ze zbieraniem danych z zewnętrznych źródeł • zagadnienia związane z eksportem danych do zewnętrznych źródeł • wykorzystywanie interfejsu API

Wymagania dotyczące certyfikowanych szkoleń producenta oferowanego oprogramowania	
SC1	Wykonawca zobowiązany jest do dostarczenia voucherów na certyfikowane szkolenia autoryzowane przez producenta oferowanego oprogramowania dla maksymalnie 5 osób. Dostarczone vouchery nie będą wystawione imiennie. Dostarczone vouchery będą miały co najmniej rok ważność na ich wykorzystanie lub będą pozwalały na bezpłatne przedłużenie ich ważności.
SC2	Certyfikowane szkolenia producenta będą omawiały wszystkie komponenty dostarczonego oprogramowania.
SC3	Językiem szkolenia musi być język polski.
SC4	Wykonawca szkolenia zapewni uczestnikom odpowiednie materiały szkoleniowe w formie elektronicznej.
SC5	Czas szkolenia: minimum 4 dni (minimum po 6 godzin dziennie). Jeżeli Wykonawca uważa, że jest potrzebny dłuższy okres na przekazanie omawianego zakresu materiału, Zamawiający dopuszcza dłuższy czas szkolenia.
SC6	Certyfikowane szkolenia producenta mogą odbyć się w formie zdalnej.
SC7	Wykonawca szkolenia przygotuje na potrzeby przeprowadzenia szkolenia wszelkie niezbędne zaplecze techniczne tj. środowiska informatyczne dla poszczególnych uczestników, wirtualną salę laboratoryjną, oprogramowanie, licencje. Każdy uczestnik szkolenia będzie miał przydzielone własne środowisko informatyczne.
SC8	Po zakończeniu certyfikowanego szkolenia producenta uczestnikom zostaną przekazane certyfikaty uczestnictwa.

Uniwersytet Rolniczy im. Hugona Kołłątaja w Krakowie
31-120 Kraków, al. Adama Mickiewicza 21
www.urk.edu.pl
NIP: 675-000-21-18 REGON: 000001815