Umowa nr.....

W dniu ..... w Warszawie pomiędzy:

Skarbem Państwa - Kasą Rolniczego Ubezpieczenia Społecznego z siedzibą w Warszawie przy Al. Niepodległości 190, 00 – 608 Warszawa, NIP 526-00-13-054, REGON 012513262, zwaną dalej „Zamawiającym",

w imieniu której występuje:

..... Biura Informatyki i Telekomunikacji na podstawie pełnomocnictwa Prezesa Kasy Rolniczego Ubezpieczenia Społecznego nr..... z dnia.....

a

..... z siedzibą....., wpisaną do rejestru przedsiębiorców Krajowego Rejestru Sądowego, prowadzonego przez .....Wydział Gospodarczy Krajowego Rejestru Sądowego pod nr KRS: , NIP: , REGON: , o kapitale zakładowym:..... zł,

zwaną dalej „Wykonawcą"

w imieniu której występuje:

.....

zwanymi dalej łącznie „Stronami"

W wyniku przeprowadzenia uproszczonego postępowania do którego na podstawie art. 4 pkt 8 ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (Dz. U. z 2019 r., poz. 1843 z późn. zm.) nie stosuje się przepisów niniejszej ustawy, zawarto umowę następującej treści:

§ 1

1. Przedmiotem umowy jest zakup wraz z dostawą licencji rozwiązania informatycznego służącego do ochrony komputerów wykorzystywanych poza siedzibą KRUS do pracy zdalnej w ilości 250 sztuk.
2. Szczegółowy opis wymagań dotyczących systemu stanowi Załącznik nr 2 do niniejszej Umowy.

§ 2

1. Wykonawca zobowiązuje się w terminie do 10 dni od daty zawarcia umowy dostarczyć Zamawiającemu dokument lub dokumenty potwierdzające udzielenie Zamawiającemu licencji na oprogramowanie wraz z usługą asysty technicznej i konserwacji producenta w zakresie wskazanym w § 1 niniejszej umowy oraz zobowiązuje się przekazać Zamawiającemu najnowsze

wersje oprogramowania, na które zostaje udzielona licencja, albo wskaże odpowiednie adresy producenta do pobrania oprogramowania.

2. Wykonawca wraz z dokumentem, o którym mowa w ustępie 1, zobowiązuje się w terminie do 10 dni od dnia zawarcia umowy, dostarczyć Zamawiającemu potwierdzenie zapewnienia asysty technicznej oprogramowania w zakresie wskazanym w § 1 niniejszej umowy. W ramach licencji Zamawiający nabędzie uprawnienia zdefiniowane przez producenta oprogramowania w ramach ww. usługi w szczególności prawa co najmniej do:
    a) pobierania od producenta w postaci elektronicznej nowych wersji posiadanego oprogramowania,
    b) pobierania od producenta poprawek i łatek do posiadanego oprogramowania,
    c) zgłaszania i uzyskiwania pomocy technicznej od producenta w zakresie problemów, wad i błędów wykrytych w oprogramowaniu bezpośrednio od producenta,
    d) dostępu do bazy wiedzy producenta w zakresie posiadanego oprogramowania.
3. Udzielenie licencji na oprogramowanie potwierdzone zostanie na piśmie, na podstawie dokumentu wystawionego przez producenta oprogramowania. Odbiór licencji nastąpi na podstawie protokołu odbioru, podpisanego „bez zastrzeżeń" przez upoważnionych przedstawicieli Wykonawcy i Zamawiającego. Formularz protokołu odbioru stanowi Załącznik nr 1 do Umowy.
4. Wykonawca zobowiązany będzie do świadczenia pomocy w rozwiązywaniu problemów związanych z użytkowaniem ww. oprogramowania i błędami powstałymi w toku jego eksploatacji. Usługi asysty technicznej i konserwacji będą świadczone co najmniej w dni robocze, w godz. 8.00-16.00.
5. Usługi asysty technicznej i konserwacji świadczone będą przez Wykonawcę co najmniej za pomocą następujących kanałów:
    a) za pomocą dedykowanego do świadczenia pomocy technicznej systemu internetowego producenta (opcjonalnie):.....
    b) telefonicznie, na numer telefonu: .....
    c) za pomocą poczty elektronicznej: .....
6. Wykonawca zobowiązany będzie do bieżącego informowania Zamawiającego o możliwościach i warunkach podnoszenia wersji posiadanego oprogramowania.
7. Poziom świadczonej usługi dla całości wyszczególnionego oprogramowania określony jest na poziomie – standard/podstawowym.

W. Bajka

§ 3

1. Wykonawca gwarantuje, że realizacja niniejszej Umowy nie spowoduje naruszenia czyichkolwiek praw autorskich, znaków handlowych, towarowych, patentów, rozwiązań konstrukcyjnych oraz innych praw chronionych.
2. Wykonawca przyjmuje na siebie wszelką odpowiedzialność za naruszenie praw osób trzecich w związku z realizacją Umowy, dotyczącą w szczególności naruszenia czyichkolwiek praw autorskich.
3. Na mocy niniejszej umowy Wykonawca, na czas nieokreślony udziela Zamawiającemu prawa do korzystania z oprogramowania określonego w § 1 na polach eksploatacji:
    a) prawo do korzystania z wszystkich funkcjonalności dostarczonego oprogramowania w dowolny sposób w liczbie kopii/ stanowisk/ serwerów/ użytkowników charakterystycznej dla dostarczonego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,
    b) prawo do instalowania dostarczonego oprogramowania w liczbie kopii/ stanowisk/ serwerów/użytkowników charakterystycznej dla odsprzedawanego oprogramowania zgodnie z opublikowanymi przez producenta warunkami licencyjnymi,
    c) prawo do instalowania wszelkich poprawek opublikowanych na stronach producenta oprogramowania oraz polach eksploatacji określonych w opublikowanych przez producenta warunkach licencyjnych.

§ 4

1. Wynagrodzenie całkowite Wykonawcy za realizację przedmiotu umowy nie przekroczy kwoty ..... zł netto (słownie złotych: .....zł 00/100) plus podatek VAT w wysokości 23%, co stanowi kwotę ..... zł brutto (słownie złotych: .....zł 00/100).
2. Ceny oprogramowania wynoszą zgodnie z tabelą:

Nazwa licencji	Ilość (sztuk)	Cena jednostkowa netto w PLN	Stawka podatku VAT w %	Wartość całkowita netto w PLN	Wartość całkowita brutto w PLN
	250		23%		

3. Wynagrodzenie, o którym mowa w ust. 1 zawiera wszystkie koszty Wykonawcy związane z realizacją przedmiotu umowy.

4. Podstawą do zapłaty faktury VAT będzie Protokół odbioru podpisany bez zastrzeżeń przez upoważnionych przedstawicieli Stron. Wzór Protokołu odbioru stanowi Załącznik nr 1 do Umowy.
5. Zapłata wynagrodzenia za wykonanie przedmiotu umowy nastąpi przelewem na rachunek bankowy Wykonawcy, wskazany w fakturze VAT, w terminie do 21 dni od dnia dostarczenia do siedziby Zamawiającego poprawnie wystawionego oryginału faktury VAT wraz z oryginałem Protokołu odbioru podpisanym bez zastrzeżeń przez upoważnionych przedstawicieli Stron.
6. Za dzień płatności przyjmuje się dzień obciążenia rachunku bankowego Zamawiającego należną Wykonawcy kwotą.
7. Zamawiający nie wyraża zgody na cesję wierzytelności wynikających z Umowy.
8. Wykonawca zobowiązany jest zamieścić na fakturze adnotację „mechanizm podzielonej płatności", jeżeli dokumentuje ona czynność podlegającą temu mechanizmowi.

(dotyczy przypadku gdy Wykonawca będzie korzystał z przesyłania faktur VAT za pośrednictwem poczty elektronicznej).

9. Zamawiający oświadcza, że zgodnie z przepisami ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług (t. j. Dz. U. z 2020r. poz. 106), wyraża zgodę na wystawienie przez Wykonawcę faktury VAT, korekt faktury VAT oraz ich duplikatów w formie elektronicznej (w formacie PDF) i przesyłanie ich za pośrednictwem poczty elektronicznej na adres: bf@krus.gov.pl. Wykonawca oświadcza, że adresem z którego będą wysyłane faktura VAT, korekty faktury VAT oraz ich duplikaty, jest następujący adres: .....

§ 5

1. W przypadku opóźnienia w dostarczeniu przez Wykonawcę, we wskazanym terminie, dokumentu lub dokumentów potwierdzających udzielenie Zamawiającemu licencji oraz wykupienie usługi, Wykonawca zapłaci Zamawiającemu karę w wysokości 1% wynagrodzenia całkowitego brutto, o którym mowa w § 4 ust.1 za każdy rozpoczęty dzień opóźnienia.
2. W przypadku odstąpienia od umowy przez Wykonawcę lub Zamawiającego z przyczyn leżących po stronie Wykonawcy, Wykonawca zapłaci Zamawiającemu karę umowną w wysokości 10% wynagrodzenia całkowitego brutto, o którym mowa w § 4 ust.1.
3. Zamawiający może dochodzić odszkodowania przewyższającego wysokość kar umownych na zasadach ogólnych.
4. Wykonawca wyraża zgodę na potrącenie kar umownych z przysługującemu mu wynagrodzenia.

§ 6

1. W czasie obowiązywania niniejszej umowy oraz przez czas nieograniczony po jej wygaśnięciu, Strony zobowiązane są zapewnić poufność informacji dotyczących drugiej Strony,

W. Bijdug

w szczególności informacji technicznych, technologicznych, ekonomicznych, finansowych, handlowych, prawnych i organizacyjnych pozyskanych w związku z wykonywaniem niniejszej umowy i nie ujawniać tych informacji bez uprzedniej zgody drugiej Strony.

2. Żadna ze Stron nie będzie, bez uprzedniej pisemnej zgody drugiej Strony kopiować, rozpowszechniać ani ujawniać komukolwiek informacji dotyczących drugiej Strony, jej interesów, finansów lub działań, włącznie z wszelkimi informacjami technicznymi, finansowymi i tajemnicą przedsiębiorstwa, niezależnie od źródeł tych informacji, chyba, że taka informacja jest już powszechnie znana bez naruszenia postanowień niniejszej umowy lub musi być ujawniona uprawnionemu organowi lub osobom, działającym w ramach obowiązujących przepisów prawa.

§ 7

1. Wszelkie zmiany Umowy wymagają formy pisemnej pod rygorem nieważności.
2. Zamawiający przewiduje możliwość zmiany postanowień zawartej umowy na zasadach określonych w art. 144 ust. 1 ustawy Prawo zamówień publicznych.

§ 8

1. Zamawiający ma prawo odstąpić od umowy w trybie natychmiastowym, w przypadku gdy Wykonawca nie zrealizuje dostawy w terminie 3 dni, licząc od dnia podpisania umowy.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowanie przepisy ustawy Prawo zamówień publicznych, ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz. U. z 2019 r. poz. 1231 z późn. zm.) oraz ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny (Dz. U. z 2019 r. poz. 1145).
3. Wszelkie ewentualne spory mogące wynikać przy realizacji niniejszej umowy będą podlegały rozstrzygnięciu przez sąd powszechny właściwy miejscowo dla siedziby Zamawiającego.
4. Integralną część umowy stanowi poniżej wymieniony załącznik.
5. Umowę sporządzono w dwóch jednobrzmiących egzemplarzach. Jeden egzemplarz dla Zamawiającego i jeden dla Wykonawcy.

Wykaz załączników:

Załącznik nr 1 - Protokół odbioru dokumentu/ów na udzielenie licencji.

Załącznik nr 2 - Wymagania dotyczące systemu (oprogramowania).

ZAMAWIAJĄCY: **WYKONAWCA:**

Załącznik nr 1

do Umowy nr .....

z dnia.....

Protokół odbioru dokumentu/ów na udzielenie licencji

W dniu.....w siedzibie Centrali KRUS w Warszawie przy Al. Niepodległości 190 dokonano odbioru dokumentu/dokumentów poświadczających udzielenie licencji na

.....

.....

250 sztuk wskazanego oprogramowania (Wykonawca wskazał adresy producenta do pobrania oprogramowania)*

Niniejszy Protokół odbioru jest podstawą do zapłaty faktury za wykonanie przedmiotu umowy.

1. Uwagi.....
   .....
   .....
2. Dostawa została przyjęta (nieprzyjęta)* ze względu na:
   .....
   .....
   .....

Zamawiający **Wykonawca**

*/ niepotrzebne skreślić

W. Bajdak

Załącznik nr 2

do Umowy nr.....

z dnia.....

Wymagania dotyczące systemu (oprogramowania)

Przedmiotem zapytania jest dostarczenie licencji oprogramowania wg opisanych wymagań oraz usługa wdrożenia systemu bezpieczeństwa.

I. Składniki architektury systemu (oprogramowania).

1. Proponowany System powinien składać się z elementów pełniących następujące funkcje:
   1.1. „Konsola zarządzająca" – do zarządzania Systemem i analizy zdarzeń.
   1.2. „agent" – instalowany na stacjach końcowych/serwerach
   1.3. „serwery danych" – system przechowujący zdarzenia/definicie/inne
2. Proponowany system musi być dostarczony w formie oprogramowania do instalacji na systemach MS Windows oraz MAC i Linux.
3. Serwery danych muszą być instalowane na lokalnych serwerach Windows oraz Linux
4. System musi być dostarczony z licencją pozwalająca na instalację *250* agentów oraz być objęte wsparciem producenta przez *12* miesięcy

II. Ochrona systemu (oprogramowania) – antymalware protection.

1. Oprogramowanie agenta musi mieć zdolność aktywnej ochrony przed złośliwym kodem za pomocą skanowania w trybie „on-access" na podstawie sygnatur
2. Oprogramowanie agenta musi mieć możliwość wykonywania skanowania na żądanie
3. Moduł ochrony przed złośliwym oprogramowaniem musi mieć możliwość wykrywania behawiorystycznego opartego o metody wykorzystywane przez złośliwy kod a działające bez sygnaturowo
4. Musi istnieć możliwość wykluczenia wskazanych katalogów, procesów, sum kontrolnych z dokładnością do grup zdefiniowanych przez użytkownika lub wskazanych z katalogu Active Directory
5. Oprogramowanie musi posiadać centralną kwarantannę
6. Oprogramowanie agenta musi współpracować poprawnie z system MS Windows w zakresie rejestracji i raportowania ochrony przed złośliwym oprogramowaniem
7. Cała opisana funkcjonalność musi być dostępna na systemy klasy MS Windows

III. Wykrywanie oraz reagowanie na nieznane zagrożenia – endpoint detection and response - EDR

1. Oprogramowanie agenta musi mieć możliwość zbierania wszystkich zdarzeń z systemów MS Windows takich jak:
    a. Zmiany w rejestrze
    b. Operacje na poziomie procesów (tworzenie, zamykanie, etc)
    c. Operacje na poziomie plików (tworzenie, kasowanie, modyfikacja, etc)
    d. Operacje na poziomie pamięci masowej podłączanej po USB
    e. Operacje na poziomie zapytań DNS
    f. Operacje na poziomie komunikacji sieciowej
    g. Wskazane zdarzenia zbierane przez log systemowy
2. Agent musi implementować reguły wykrywania potencjalnych nowych zagrożeń na poziomie analizy zbieranych zdarzeń opisanych powyżej ,
3. Reguły behawiorystyczne muszą być dostarczane i tworzone przez producenta systemu
4. Musi istnieć możliwość tworzenia reguł własnych np. na podstawie zebranych zdarzeń
5. Musi istnieć możliwość zbierania zdarzeń tylko w oknie wystąpienia alarmu tj 2 minuty przed oraz po alarmie. Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręczenie bądź z Active Directory
6. Agent musi umożliwiać szereg reakcji uruchamianych ręcznie bądź automatycznie na podstawie generowanych alarmów, takich jak:
    a. Analiza pamięci
    b. Zrzut pamięci oraz zrzut obrazu dysku
    c. Zebranie wskazanego pliku
    d. Przeszukanie rejestru
    e. Zebranie informacji z ARP cache
    f. Zebranie informacji z DNS Cache
    g. Odtworzenie systemu operacyjnego w całości
    h. Powrót do ostatniej dobrej konfiguracji
    i. Zakończenie wskazanego procesu
    j. Lista zalogowanych użytkowników
    k. Zebranie informacji o zadaniach, ustawieniach autorun, etc
7. Musi istnieć możliwość tworzenia własnych zadań wykonywanych przez agenta w formie skryptu wraz z ewentualnymi narzędziami potrzebnymi do jego wykonania

W. Kajdan

8. Musi istnieć możliwość ręcznej oraz automatycznej izolacji hosta na skutek wykrytego zdarzenia.
9. Musi istnieć możliwość określenia adresów IP zaufanych serwerów z którymi komunikacja jest zawsze dozwolona (np. Active Directory/SCCM/etc)
10. Agent musi pozwalać na blokowanie uruchamiania się procesów o wskazanych sumach kontrolnych. Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręczenie bądź z Active Directory
11. Agent musi pozwalać na odkładanie każdej nowej instancji kodu wykonywalnego widzianego pierwszy raz w środowisku nawet jeżeli kod ten nie zostanie zapisany w formie pliku na dysku (np. skrypt uruchamiany w pamięci). Ustawienie to musi być dostępne z dokładnością do stacji bądź grupy agentów stworzoną ręczenie bądź z Active Directory
12. Agent musi pozwalać na uruchamianie i analizę plików YARA oraz IOC. Producent musi udostępniać uaktualnianą listę plików oraz musi istnieć możliwość wskazania serwera z własnymi listami. Musi również być możliwość importu własnych plików.
13. Agent musi zbierać informacje o zainstalowanym oprogramowaniu na hoście oraz korelować ją z listą aktualnych znanych podatności (CVE) wskazując istniejące podatności na każdym z hostów
14. Cała opisana funkcjonalność musi być dostępna na systemy klasy MS Windows
15. Dla systemów klasy MAC oraz Linux system musi oferować co najmniej możliwość odpowiedzi opisanych w punkcie 6.

IV. Zarządzanie Systemem (oprogramowaniem)

1. System musi pozwalać na zarządzanie wszystkimi komponentami dokonującymi analizy oraz wszystkimi ich parametrami takimi, jak: konfiguracja trybów pracy, tworzenie reguł/polityk bezpieczeństwa, konfigurację zasad alarmowania, zasad eksportu danych do innych systemów bezpieczeństwa, zasad wykonywania kopii bezpieczeństwa, propagowanie poprawek i aktualizacje oprogramowania, zarzadzanie licencjami przy pomocy komponentu realizującego funkcję centralnego systemu zarządzania
2. Korzystanie z centralnego systemu zarządzania musi odbywać się przy pomocy jednego interfejsu graficznego dostępnego zdalnie, przy wykorzystaniu przeglądarki internetowej.
3. Komunikacja służąca zapewnieniu zdalnego dostępu użytkowników i administratorów do Systemu jak również pomiędzy poszczególnymi jego komponentami musi być zabezpieczona kryptograficznie w zakresie zapewnienia poufności i integralności przesłanych danych.
4. Centralny system zarządzania musi pozwalać na tworzenie kont użytkowników Systemu o różnych poziomach uprawnień. W zakresie uwierzytelniania użytkowników Systemu wymagana jest możliwość integracji z LDAP/AD.

5. W ramach konsoli zarządzającej, dla wszystkich obsługiwanych przez nią komponentów, musi być dostępna funkcjonalność wewnętrznego audytu, umożliwiająca logowanie i przegląd wszystkich działań
6. Musi istnieć możliwość integracji z systemami klasy SIEM celem wysyłania informacji o zdarzeniach do dalszej korelacji
7. Musi istnieć możliwość integracji poprzez API z systemami SOAR celem automatyzacji konfiguracji
8. Musi istnieć możliwość integracji z systemami klasy SIEM w sposób umożliwiający operatorom SIEM wykonywanie podstawowych zadań agenta bezpośrednio z konsoli SIEM (np. analiza procesów).

Wymagania dotyczące kompetencji zespołu wdrożeniowego:

Kierownik zespołu wdrożeniowego:

- kompetencje z obszaru bezpieczeństwa IT, w szczególności związane z technikami ofensywnymi oraz dobrymi praktykami wynikającymi z wiedzy audytorskiej (z uwagi na charakter poszukiwanego rozwiązania) potwierdzone co najmniej certyfikatami:
- ISC2 CISSP,
- CISA,
- EC-Council Certified Ethical Hacker CEH,
- Offensive Security OSCE

Zamawiający będzie wymagał kopii certyfikatów na etapie oceny ofert.

Dodatkowo, wykonawca powinien dysponować min. 2 osobowym zespołem ekspertów bezpieczeństwa, którzy będą świadczyć usługę utrzymania systemu i analizy incydentów bezpieczeństwa. Każdy członek zespołu powinien posiadać najwyższy poziom certyfikacji producenta oferowanego rozwiązania.

Zamawiający będzie wymagał kopii certyfikatów na etapie oceny ofert.

W. Bajtka