Projekt **ZAŁĄCZNIK NR 1 DO SIWZ**

UMOWA NR BDG.zp.23.1.83.2018

zawarta w dniu ..... w Warszawie

pomiędzy

Skarbem Państwa - Ministerstwem Rolnictwa i Rozwoju Wsi, ul. Wspólna 30, 00-930 Warszawa, NIP 526-12-81-638, REGON 000063880, zwanym dalej **„Kupującym”**, reprezentowanym przez Panią Monikę Rzepecką, Dyrektora Generalnego Ministerstwa Rolnictwa i Rozwoju Wsi,

a

……..,
zwaną dalej **”Sprzedawcą”**, reprezentowaną przez …….,

o następującej treści:

§ 1.

1. W ramach umowy Sprzedawca zobowiązuje się:
   1) przenieść na Kupującego własność i wydać mu System ochrony stacji roboczych i serwerów, zwany dalej „Systemem”,
   2) wykonać wdrożenie i integrację Systemu z infrastrukturą teleinformatyczną Kupującego,
   3) zapewnić udzielenie Kupującemu niewyłącznej licencji na okres 12 miesięcy na korzystanie z Systemu, zwanej dalej „licencją”,
   4) zapewnić wsparcie techniczne dla Systemu, na okres 12 miesięcy i dostarczyć stosowne dokumenty, potwierdzające prawo do korzystania przez Kupującego z usługi wsparcia technicznego i aktualizacji dla Systemu.
2. Szczegółowy opis Systemu stanowi załącznik do umowy.

§ 2.

1. Sprzedawca zobowiązuje się dostarczyć System, dokument potwierdzający udzielenie Kupującemu licencji, dokument potwierdzający prawo do korzystania przez Kupującego z usługi wsparcia technicznego i aktualizacji do siedziby Kupującego na własny koszt oraz wykonać wdrożenie i integrację Systemu, o których mowa w § 1 ust. 1 pkt 2, w terminie do ……dni od dnia zawarcia umowy.
2. Kupujący dokona odbioru Systemu i dokumentów, o których mowa w ust. 1, oraz potwierdzi wykonanie wdrożenia i integracji, o których mowa w § 1 ust. 1 pkt 2, na podstawie protokołu zdawczo-odbiorczego.

§ 3.

W ramach udzielonej licencji, o której mowa w § 1 ust. 1 pkt 3, Kupujący jest upoważniony do korzystania z Systemu zgodnie z jego przeznaczeniem.

§ 4.

1. Za System, wdrożenie i integrację, licencję, usługę wsparcia technicznego i aktualizacji, o których mowa w § 2 ust. 1, Kupujący zapłaci Sprzedawcy cenę w wysokości ..... zł brutto (słownie: .....zł), w tym 23% VAT.

2. Zapłata ceny nastąpi na podstawie faktury VAT prawidłowo wystawionej przez Sprzedawcę, na wskazany przez niego rachunek bankowy, w terminie 21 dni od dnia doręczenia prawidłowo wystawionej faktury VAT Kupującemu.
3. Za dzień zapłaty ceny uważa się dzień obciążenia rachunku bankowego Kupującego.
4. Wystawienie faktury VAT przez Sprzedawcę nastąpi po dokonaniu przez Kupującego odbioru i potwierdzenia, o których mowa w § 2 ust. 2.

§ 5.

1. W przypadku:
   1) zwłoki w wykonaniu umowy albo jej części, Sprzedawca zapłaci na rzecz Kupującego karę umowną w wysokości 1% ceny określonej w § 4 ust. 1, za każdy dzień zwłoki, nie więcej jednak niż 10% tej ceny;
   2) nienależytego wykonania umowy albo jej części, Sprzedawca zapłaci na rzecz Kupującego karę umowną w wysokości 10% ceny określonej w § 4 ust. 1.
2. W razie zwłoki, o której mowa w ust. 1 pkt 1, powyżej 15 dni, Kupującemu przysługuje prawo odstąpienia od umowy albo jej części.
3. Odstąpienie od umowy nie powoduje utraty prawa dochodzenia przez Kupującego kary umownej.
4. W przypadku, gdy wysokość szkody poniesionej przez Kupującego przewyższa wysokość zastrzeżonej kary umownej, Sprzedawca jest zobowiązany do naprawienia szkody w pełnej wysokości.

§ 6.

Wszelkie zmiany niniejszej umowy wymagają formy pisemnej pod rygorem nieważności.

§ 7.

W sprawach nieuregulowanych niniejszą umową mają do niej zastosowanie przepisy Kodeksu cywilnego.

§ 8.

Spory wynikłe w związku z realizacją niniejszej umowy rozstrzygane będą przez sąd właściwy dla siedziby Kupującego.

§ 9.

Umowę sporządzono w 4 jednobrzmiących egzemplarzach, z których 3 egzemplarze otrzymuje Kupujący, a 1 egzemplarz Sprzedawca.

KUPUJĄCY	**SPRZEDAWCA**
……..	……..

Załącznik do umowy
nr BDG.zp.23.1.83.2018
z dnia ……..……

Szczegółowy opis Systemu ochrony stacji roboczych i serwerów

1. System ochrony stacji roboczych i serwerów:

Producent Systemu:		……
Nazwa Systemu:		……
Lp.	**Opis wymagań minimalnych**	**Deklaracja zgodności z opisem wymagań minimalnych (Tak / Nie)**
1.	Możliwość zabezpieczenia co najmniej 1000 stacji roboczych i 100 serwerów.	
2.	Funkcjonowanie współbieżne z innymi rozwiązaniami zabezpieczeń stacji roboczych, wykorzystywanymi przez Zamawiającego w szczególności Symantec Endpoint Protection, w zakresie ochrony przed atakami aplikacyjnymi oraz złośliwymi kodami wykonywalnymi.	
3.	Zarządzanie poprzez graficzny interfejs użytkownika typu Web (Web GUI).	
4.	3-warstwowa architektura składająca się z konsoli, serwera zarządzania oraz serwera bazy danych. Instalacja i uruchomienie wszystkich trzech komponentów jest możliwe na jednym serwerze sprzętowym lub w architekturze rozproszonej.	
5.	Instalacja wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli.	
6.	Eksport logów w standardzie syslog do dowolnego zewnętrznego systemu zarządzania logów.	
7.	Rozwiązanie programowe działające na serwerowych systemach operacyjnych, w szczególności Windows Server 2012 R2.	
8.	Możliwość uruchomienia w środowisku zwirtualizowanym VMware.	
9.	Zapewnienie ochrony procesów i aplikacji z możliwością dodawania do listy chronionych procesów aplikacji własnych.	
10.	Funkcja monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznanie procesów i aplikacji działających na stacjach końcowych użytkowników) celem uruchomienia wdrożenia pilotażowego.	
11.	Ochrona w czasie rzeczywistym przed możliwością wykorzystania jakiegokolwiek błędu bezpieczeństwa aplikacji poprzez blokowanie technik wykonania ataku.	
12.	Zapewnienie, poprzez blokowanie technik ataków, skutecznej ochrony przed atakami wykonywanymi	

	z użyciem exploit'ów dnia zerowego lub exploit'ów nieznanych, wykorzystujących dowolny błąd bezpieczeństwa aplikacji.	
13.	Możliwość monitorowania i zapobiegania atakom poprzez blokowanie szeregu technik ataków bez konieczności połączenia do serwera zarządzania i/lub usługi chmurowej i nie bazując na metodzie sygnaturowej.	
14.	W przypadku wykrycia techniki ataku ukierunkowanej na podatną aplikację, celem zablokowania ataku następuje zatrzymanie proces atakowanej aplikacji, zebranie pełnego zestawu danych dowodowych (takich jak nazwa atakowanego procesu, źródło pochodzenia pliku, znacznik czasowy, zrzut pamięci, wersja systemu operacyjnego, tożsamość użytkownika, wersja podatnej aplikacji, itp.) oraz zakończenie działania tylko tego konkretnego procesu.	
15.	Wykorzystywanie modułów zapobiegania i blokowania technik ataków. Działanie nie może być oparte o metodę sygnaturową, reputacyjną lub analizę heurystyczną pliku. Możliwość zastosowania modułów blokowania technik ataków zarówno dla powszechnie znanych i popularnych aplikacji jak i aplikacji własnych.	
16.	Wykorzystywane zasoby sprzętowe chronionego komputera: – użycie procesora nie więcej niż 1% – użycie pamięci RAM nie więcej niż 50MB.	
17.	Jednoczesna ochrona wszystkich aplikacji i procesów przed wszystkimi technikami ataków.	
18.	Tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych i działających na nich procesów bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów.	
19.	Ochrona przed uruchomieniem złośliwych plików wykonywalnych.	
20.	Funkcja monitorowania i uczenia się środowiska aplikacyjnego Zamawiającego (tj. rozpoznanie procesów i aplikacji działających na stacjach końcowych użytkowników).	
21.	Pełna kontrola i ustalanie restrykcji parametrów i sposobu uruchamiania plików wykonywalnych (np. dozwolone foldery źródłowe, ścieżki sieciowe, urządzenia zewnętrzne, możliwość uruchamianie plików nie posiadających podpisu cyfrowego wystawcy, możliwość tworzenia procesów potomnych, itp.).	
22.	Zapobieganie uruchamianiu złośliwego oprogramowania poprzez użycie modułów blokujących typowe zachowania złośliwych kodów wykonywalnych.	
23.	Konfiguracja globalnych list dozwolonych plików wykonywalnych w środowisku Zamawiającego.	
24.	Tworzenie wyjątków konfiguracyjnych dla określonych stacji końcowych celem wykluczenia ich z ogólnych reguł ochrony bezpośrednio z poziomu i na bazie zebranych po stronie konsoli zarządzającej logów.	
25.	Ochrona przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.	

26.	Możliwość weryfikacji w chmurowym środowisku anty-APT (Advanced Persistent Threat) czy dany plik jest złośliwy, czy legalny na bazie skrótu cyfrowego pliku.	
27.	Możliwość wysłania poprzez serwer zarządzania potencjalnie złośliwego pliku do analizy w chmurowym środowisku anty-APT.	
28.	Możliwość wglądu w raport wynikowy analizy pliku w środowisku chmurowym anty-APT bezpośrednio z poziomu stacji zarządzania oprogramowaniem zabezpieczeń stacji końcowych.	
29.	Zapobieganie nieznanym złośliwym plikom wykonywalnym poprzez zastosowanie chmurowego środowiska anty-APT typu "sandbox". Możliwość przedstawienia wyniku analizy pliku wraz z pełnym raportem z analizy.	
30.	Możliwość ręcznego dostrojenia lub nadpisania werdyktu będącego wynikiem analizy w środowisku chmurowym dla konkretnego skrótu cyfrowego pliku.	
31.	Możliwość zablokowania uruchomienia pliku wykonywalnego jeśli skrót cyfrowy pliku jest nieznany, tj. plik ten nie był uprzednio analizowany w środowisku chmurowym anty-APT producenta.	
32.	Możliwość uruchomienia analizy statycznej pliku opartej o algorytmy uczenia.	
33.	Wbudowane pulpity raportów (ang. Dashboard) do monitorowania poziomu i stanu bezpieczeństwa środowiska Zamawiającego (tj. Pulpit Stanu Komponentów Systemu, Pulpit Zdarzeń Bezpieczeństwa, Pulpit Szczegółowego Dziennika Zagrożeń, Pulpit Szczegółowego Dziennika Błędów Bezpieczeństwa).	
34.	Wbudowane pulpity raportów (ang. Dashboard) do monitorowania stanu poszczególnych stacji końcowych Zamawiającego (tj. Pulpit Szczegółowego Stanu/Statusu Stacji Końcowych, Pulpit Historii Reguł Bezpieczeństwa Stacji Końcowych, Pulpit Zmian Reguł Bezpieczeństwa Stacji Końcowych, Pulpit Historii Stanu Serwisu Stacji Końcowych).	
35.	Wyświetlanie informacji za pomocą przeglądarki www, na temat wykrytych zagrożeń i złośliwego oprogramowania oraz eksport dziennika zdarzeń zagrożeń i stanu stacji końcowych w formacie CSV.	
36.	Możliwość zbierania dokumentacji dowodowej i danych ze stacji końcowych w jednym centralnym punkcie.	
37.	Możliwość zbierania informacji w celu przeprowadzenia późniejszej analizy, w szczególności takich jak: Zrzut pamięci (Memory Dump), Otwarte pliki, Załadowane moduły, Otwarte URI, Procesy nadrzędne).	
38.	Możliwość użycia usługi inteligentnego transferu w tle - BITS (Background Intelligence Transfer Service) przy wykorzystaniu przeglądarki web oraz możliwość przesyłania danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego.	
39.	Możliwość dostosowania polityk powiązanych z dokumentacją dowodową w ramach serwera	

	zarządzającego, w celu zdefiniowania jaki typ danych powinien zostać zebrany w przypadku wystąpienia incydentu.	
40.	Wyświetlenie wysokopoziomowych informacji systemowych na temat stacji końcowej po wykryciu zagrożenia oraz możliwość zebrania danych odnoszących się do zastosowanego mechanizmu ochrony celem dalszej analizy i śledztwa.	
41.	Automatyczne tworzenie wyjątków odnośnie reguł oraz skrótów cyfrowych bezpośrednio z raportu dotyczącego wykrytego zagrożenia w celu umożliwienia uruchomienia danego procesu na poszczególnych stacjach końcowych.	

2. Wdrożenie i integracja:

1. Instalacja i konfiguracja Systemu ochrony stacji roboczych i serwerów w środowisku Zamawiającego.
2. Konfiguracja oprogramowania bazy danych (Microsoft SQL Server) niezbędnego do poprawnego funkcjonowania Systemu.
3. Integracja z posiadanym przez Zamawiającego CA (Certificate Authority).
4. Przygotowanie zdalnej instalacji klientów Systemu na wskazanych przez Zamawiającego stacjach roboczych, w celu sprawdzenia false-positives i dostosowania odpowiednich reguł i polityk.
5. Przygotowanie i konfiguracja GPO (Group Policy Objects) w usłudze katalogowej Active Directory do automatycznej instalacji klientów na wszystkich stacjach roboczych i serwerach.