Nr sprawy: FZ-1/5097/MKO/18 **Katowice, 31/10/2018 r.**

Dotyczy : Wstępnego zapytania ofertowego w celu ustalenia wartości zamówienia dla planowanego postępowania przetargowego

Szanowni Państwo,

Zwracamy się z prośbą o wstępną ofertę na dostawę 1000 szt. 3 letniej licencji oprogramowania antywirusowego dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z sandboxingiem w chmurze i wsparciem technicznym.

WYMAGANIA OGÓLNE
Wymagana funkcjonalność oprogramowania

Typ oferowanej licencji powinien uwzględniać status Zamawiającego – instytut badawczy podporządkowany Ministrowi Energii.

Zakres wsparcia technicznego:

- prawo do aktualizacji oprogramowania do nowszych wersji w trakcie obowiązywania licencji;
- wsparcie dostępne w dni robocze drogą mailową oraz telefoniczną (w godzinach od 8:00 do 18:00);
- pomoc techniczna w zakresie konfiguracji i administracji produktem oraz obejmująca rozwiązywanie typowych problemów z oprogramowaniem;
- wsparcie techniczne do oprogramowania świadczone w języku polskim, autoryzowane przez producenta oprogramowania.

Wymóg wdrożenia oprogramowania

Wykonawca wdroży system antywirusowy u Zamawiającego. Wdrożenie obejmuje: instalację serwera/konsoli zarządzania, deinstalacja istniejących instancji oprogramowania ESET Endpoint Antivirus Suite PL u Zamawiającego (środowisko nie jest zarządzane zdalnie, a więc nie jest w domenie), przeszkolenie personelu technicznego w zakresie użytkowania, zarządzania oraz administrowania programem. Wdrożenie oprogramowania wraz ze szkoleniami (czas trwania szkoleń - minimum: 16h) musi być przeprowadzone maksymalnie w ciągu 2 tygodni od podpisania umowy.

Zamawiający korzysta obecnie z 1 000 licencji ESET Endpoint Antivirus Suite PL ważnych do 22.12.2018 r.

Niniejszym oferujemy dostawę oprogramowania spełniającego poniższe wymagania techniczne:	
Wymagane oprogramowanie komputerowe: oprogramowanie antywirusowe dla stacji roboczych, serwerów plików i urządzeń mobilnych wraz z *sandboxingiem* w chmurze, subskrypcją wzorców wirusów i wsparciem technicznym – 1 000 sztuk 3-letniej licencji.	**Oferowane oprogramowanie komputerowe:** ..... **/należy podać pełną nazwę oprogramowania/**

Lp.	Funkcje i warunki techniczne oprogramowania komputerowego	Warunek
1	2	3
	Wymagania dla ochrony antywirusowej:	
1	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami.	**Wymagane**
2	Wykrywanie i usuwanie niebezpiecznych aplikacji typu *adware*, *spyware*, *dialer*, *phishing*, narzędzi hakerskich i *backdoor*.	**Wymagane**
3	Wbudowana technologia do ochrony przed narzędziami typu *rootkit*.	**Wymagane**
4	Wykrywanie potencjalnie niepożądanych, niebezpiecznych oraz podejrzanych aplikacji.	**Wymagane**
5	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików.	**Wymagane**

6	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	**Wymagane**
7	Możliwość utworzenia wielu różnych zadań skanowania według harmonogramu (w tym: po zalogowaniu i po uruchomieniu komputera). Każde zadanie ma mieć możliwość uruchomienia z innymi ustawieniami (m.in. metody skanowania, obiekty skanowania, czynności, rozszerzenia plików, priorytet skanowania).	**Wymagane**
8	Możliwość skanowania dysków sieciowych i dysków przenośnych.	**Wymagane**
9	Skanowanie plików spakowanych i skompresowanych.	**Wymagane**
10	Mechanizm wykluczeń: • Możliwość umieszczenia na liście wykluczeń ze skanowania wybranych plików, katalogów lub plików o określonych rozszerzeniach; • Wykluczenie ze skanowania musi odbywać się nie tylko po nazwie pliku, ale również ma być możliwe użycie symbolu wieloznacznego „*".	**Wymagane**
11	Możliwość automatycznego wyłączenia komputera po zakończonym skanowaniu.	**Wymagane**
12	Brak konieczności restartu komputera po instalacji programu.	**Wymagane**

13	Włączenie i wyłączenie ochrony: • Użytkownik musi posiadać możliwość tymczasowego wyłączenia ochrony na czas co najmniej 10 minut lub do ponownego uruchomienia komputera; • W momencie tymczasowego wyłączenia ochrony antywirusowej użytkownik musi być poinformowany o takim fakcie odpowiednim powiadomieniem i informacją w interfejsie aplikacji; • Ponowne włączenie ochrony antywirusowej nie może wymagać od użytkownika ponownego uruchomienia komputera.	**Wymagane**
14	Możliwość przeniesienia zainfekowanych plików i załączników poczty w bezpieczny obszar dysku (do katalogu kwarantanny) w celu dalszej kontroli. Pliki muszą być przechowywane w katalogu kwarantanny w postaci zaszyfrowanej.	**Wymagane**
15	Skanowanie i oczyszczanie poczty przychodzącej POP3 i IMAP "w locie" (w czasie rzeczywistym), zanim zostanie dostarczona do klienta pocztowego zainstalowanego na stacji roboczej (niezależnie od konkretnego klienta pocztowego).	**Wymagane**
16	Blokowanie możliwości przeglądania wybranych witryn internetowych. Listę blokowanych stron internetowych określa administrator.	**Wymagane**
17	Program ma umożliwiać skanowanie ruchu sieciowego wewnątrz szyfrowanych protokołów HTTPS, POP3S, IMAPS.	**Wymagane**
18	Możliwość zgłoszenia witryny z podejrzeniem zagrożenia typu *phishing* z poziomu interfejsu użytkownika w celu analizy przez laboratorium producenta.	**Wymagane**
19	Program musi posiadać funkcjonalność, która na bieżąco będzie odpytywać serwery producenta o znane i bezpieczne procesy uruchomione na komputerze użytkownika.	**Wymagane**
20	Użytkownik musi posiadać możliwość przesłania pliku celem zweryfikowania jego reputacji bezpośrednio z poziomu menu kontekstowego.	**Wymagane**
21	Wbudowane niezależne moduły heurystyczne wykorzystujące pasywne metody heurystyczne, aktywne metody heurystyczne oraz elementy sztucznej inteligencji. Możliwość automatycznego wysyłania nowych wykrytych zagrożeń do laboratoriów producenta bezpośrednio z programu (nie wymaga ingerencji użytkownika).	**Wymagane**
22	Program ma mieć możliwość kontroli zainstalowanych aktualizacji systemu operacyjnego i w przypadku braku jakiejś aktualizacji – poinformować o tym użytkownika i administratora wraz z listą niezainstalowanych aktualizacji.	**Wymagane**
23	Program ma umożliwiać administratorowi blokowanie zewnętrznych nośników danych na stacji w tym przynajmniej: pamięci masowych, optycznych pamięci masowych, pamięci masowych *firewire*, urządzeń do tworzenia obrazów, drukarek USB, urządzeń *bluetooth*, czytników kart inteligentnych, modemów, portów LPT/COM i urządzeń przenośnych.	**Wymagane**

24	Program musi być wyposażony w system zapobiegania włamaniom działający na hoście (ang. HIPS – *Host-Based Intrusion Prevention System*). Tworzenie reguł dla modułu HIPS musi odbywać się co najmniej w oparciu o: aplikacje źródłowe, pliki docelowe, aplikacje docelowe oraz elementy docelowe rejestru systemowego. Użytkownik na etapie tworzenia reguł dla modułu HIPS musi posiadać możliwość wybrania jednej z trzech akcji: *pytaj, blokuj, zezwól.*	**Wymagane**
25	Program musi być wyposażony w mechanizm ochrony przed programami typu *exploit* wykorzystującymi błędy w aplikacjach.	**Wymagane**
26	Program ma oferować funkcję, która aktywnie monitoruje i skutecznie blokuje działania wszystkich plików programu, jego procesów, usług i wpisów w rejestrze przed próbą ich modyfikacji przez aplikacje trzecie.	**Wymagane**
27	Automatyczna, inkrementacyjna aktualizacja baz wirusów i innych zagrożeń dostępna z Internetu.	**Wymagane**
28	Program musi posiadać funkcjonalność tworzenia repozytorium aktualizacji.	**Wymagane**

29	Program musi być wyposażony w funkcjonalność umożliwiającą tworzenie kopii wcześniejszych aktualizacji w celu ich późniejszego przywrócenia (ang. *rollback*).	**Wymagane**
30	Program musi być wyposażony w jeden wspólny skaner uruchamiany w pamięci, z którego korzystają wszystkie funkcje systemu (antywirus, *anti-spyware*, metody heurystyczne).	**Wymagane**
31	Program musi być wyposażony w dziennik zdarzeń rejestrujący informacje na temat znalezionych zagrożeń, kontroli witryn Internetowych i kontroli urządzeń, skanowania na żądanie i według harmonogramu, dokonanych aktualizacji baz wirusów i samego oprogramowania.	**Wymagane**
32	W programie musi istnieć możliwość tymczasowego wstrzymania polityk wysłanych z poziomu serwera zdalnej administracji. Wstrzymanie polityk ma umożliwić lokalną zmianę ustawień programu na stacji końcowej. Funkcja wstrzymania polityki musi być realizowana tylko przez określony czas, po którym automatycznie zostają przywrócone dotychczasowe ustawienia.	**Wymagane**
33	Program musi umożliwiać ochronę przed przyłączeniem komputera do sieci BOTNET.	**Wymagane**
34	Program musi posiadać funkcjonalność skanera UEFI, który chroni użytkownika poprzez wykrywanie i blokowanie zagrożeń, atakujących jeszcze przed uruchomieniem systemu operacyjnego.	**Wymagane**
35	Program musi posiadać system ochrony przed atakami sieciowymi (IDS).	**Wymagane**
36	Administrator musi posiadać możliwość dodawania wyjątków dla systemu IDS, co najmniej w oparciu o występujący alert, kierunek, aplikacje, czynność oraz adres IP.	**Wymagane**
	Wymagania dla ochrony serwerów plików MS Windows:	
37	Wsparcie dla systemów operacyjnych: Microsoft Windows Server 2008, 2008 R2, 2012, 2012 R2, 2016.	**Wymagane**
38	Instalator musi umożliwiać wybór wersji językowej programu, przed rozpoczęciem procesu instalacji.	**Wymagane**
39	Pełna ochrona przed wirusami, trojanami, robakami i innymi zagrożeniami. Wykrywanie i usuwanie niebezpiecznych aplikacji.	**Wymagane**
40	Skanowanie w czasie rzeczywistym otwieranych, zapisywanych i wykonywanych plików	**Wymagane**
41	Możliwość skanowania całego dysku, wybranych katalogów lub pojedynczych plików "na żądanie" lub według harmonogramu.	**Wymagane**
42	System antywirusowy ma mieć możliwość wykorzystania wielu wątków skanowania w przypadku maszyn wieloprocesorowych.	**Wymagane**
43	Możliwość skanowania dysków sieciowych i dysków przenośnych.	**Wymagane**
44	W przypadku wykrycia zagrożenia, ostrzeżenie może zostać wysłane do użytkownika i/lub administratora poprzez e-mail.	**Wymagane**
45	Możliwość zabezpieczenia programu przed deinstalacją przez niepowołaną osobę, nawet, gdy posiada ona prawa lokalnego lub domenowego administratora, przy próbie deinstalacji program ma pytać o hasło.	**Wymagane**

	Wymagania dla administracji zdalnej:	
46	Rozwiązanie ma być w pełni zgodne z rozporządzeniem RODO.	**Wymagane**
47	Serwer administracyjny musi oferować możliwość instalacji na systemach MS Windows Server 2008, 2012, 2016 oraz systemach Linux.	**Wymagane**
48	Musi istnieć możliwość pobrania ze strony producenta serwera zarządzającego w postaci gotowej maszyny wirtualnej w formacie OVA (ang. *Open Virtual Appliance*).	**Wymagane**
49	Serwer administracyjny musi wspierać instalację w oparciu o co najmniej bazy danych MS SQL i MySQL, posiadane przez Zamawiającego.	**Wymagane**
50	Konsola administracyjna musi umożliwiać podgląd szczegółów dotyczących bazy danych takich jak: serwer bazy danych, nazwę bazy danych, aktualny rozmiar bazy danych i nazwę hosta bazy danych.	**Wymagane**
51	Serwer administracyjny musi oferować możliwość konfiguracji zadania cyklicznego czyszczenia bazy danych.	**Wymagane**

52	Serwer administracyjny musi oferować możliwość wykorzystania już istniejących baz danych MS SQL lub MySQL, posiadanych przez Zamawiającego.	**Wymagane**
53	Narzędzie administracyjne musi wspierać połączenia poprzez serwer proxy występujące w sieci.	**Wymagane**
54	Konsola musi umożliwiać zarządzanie wszystkimi rozwiązaniami producenta zabezpieczającymi przed zagrożeniami	**Wymagane**
55	Komunikacja pomiędzy poszczególnymi modułami serwera musi być zabezpieczona za pomocą certyfikatów.	**Wymagane**
56	Centralna konfiguracja i zarządzanie ochroną antywirusową, *anti-spyware*, zaporą osobistą i kontrolą dostępu do witryn internetowych zainstalowanymi na stacjach roboczych w sieci.	**Wymagane**
57	Zarządzanie oprogramowaniem zabezpieczającym na stacjach roboczych musi odbywać się za pośrednictwem dedykowanego agenta.	**Wymagane**
58	Instalacja agenta musi odbywać się przy wykorzystaniu repozytorium producenta. Repozytorium powinno zawierać aktualne wersje agentów bez względu na rodzaj systemu operacyjnego.	**Wymagane**
59	Administrator musi otrzymywać powiadomienia o dostępnych aktualizacjach z poziomu konsoli administracyjnej	**Wymagane**
	Wymagania dla *sandboxingu* w chmurze:	
60	Zapewniać ochronę przed zagrożeniami typu *zero–day*.	**Wymagane**
61	Pozwolić na określenie, jakie typy plików mają zostać przesłane do chmury.	**Wymagane**
62	Umożliwiać administratorowi zdefiniowanie, po jakim czasie przesłane pliki muszą zostać usunięte z serwerów producenta.	**Wymagane**
63	Umożliwiać administratorowi zdefiniowanie maksymalnego rozmiaru przesyłanych próbek.	**Wymagane**
64	Pozwalać na utworzenie listy wyłączeń określonych plików lub folderów z przesyłania.	**Wymagane**
65	Po zakończonej analizie pliku, rozwiązanie musi przesyłać wynik analizy do wszystkich wspieranych produktów.	**Wymagane**
66	Pozwalać administratorowi na podejrzenie listy plików, które zostały przesłane do analizy i przez kogo.	**Wymagane**
67	Działać bez instalacji dodatkowego agenta na stacjach roboczych.	**Wymagane**
68	Pozwalać na wysłanie dowolnej próbki do analizy przez użytkownika lub administratora.	**Wymagane**
69	Przeanalizować nowe, wcześniej nie przesyłane próbki w mniej niż 5 minut.	**Wymagane**
70	Przeanalizowane pliki odpowiednio oznaczyć tak, aby jednoznacznie można było stwierdzić, czy plik jest bezpieczny czy nie.	**Wymagane**
	Wymagania dla ochrony urządzeń mobilnych:	

71	**Posiadać ochronę antywirusową umożliwiającą:** • Ochrona plików w czasie rzeczywistym; • Ochrona przed atakami typu *phishing*; • Skanowanie dostępnego w urządzeniu nośnika pamięci SD; • Aplikacja musi zapewniać co najmniej 2 poziomy dokładności skanowania; • Ochrona proaktywna wykrywająca nieznane zagrożenia; • Aplikacja ma mieć możliwość określenia domyślnej akcji podejmowanej w przypadku wykrycia zagrożenia; • Aplikacja musi umożliwiać automatyczne uruchamianie skanowania, gdy urządzenie jest w trybie bezczynności.	**Wymagane**
72	**Wykonywać skanowanie na żądanie:** • Aplikacja ma mieć możliwość skanowania zainstalowanych aplikacji; • Aplikacja ma wykorzystywać do skanowania metody heurystyczne wykrywające nieznane zagrożenia; • Informacje o skanowaniu mają być przechowywane w plikach dziennika; • Użytkownik ma mieć możliwość wymuszenia przeskanowania całego urządzenia, lub wskazania folderu, który ma być przeskanowany.	**Wymagane**

73	**Posiadać filtr SMS/MMS i połączeń (jeśli system zezwala):** • Użytkownik musi mieć możliwość definiowania własnych reguł dotyczących połączeń oraz wiadomości SMS/MMS bez konieczności podawania hasła administratora. Reguły zdefiniowane przez administratora (w trybie administratora) muszą mieć wyższy priorytet niż reguły użytkownika; • Użytkownik i administrator ma mieć możliwość tworzenia białej i czarnej listy numerów telefonów; • Użytkownik i administrator ma mieć możliwość dodania numeru telefonu, dla którego można określić akcje dla: a. Przychodzącej wiadomości SMS b. Przychodzącej wiadomości MMS c. Połączenia wychodzącego d. Połączenia przychodzącego; • Aplikacja ma mieć możliwość blokowania anonimowych połączeń przychodzących (pochodzących z ukrytych ID).	**Wymagane**
74	**Umożliwiać ochronę przed kradzieżą:** • Użytkownik ma mieć możliwość wprowadzenia zaufanej karty SIM.w oparciu o kartę wprowadzoną w danym urządzeniu lub w oparciu o dane wprowadzone ręcznie; • W przypadku kradzieży urządzenia, prawowity użytkownik ma mieć możliwość wysłania na urządzenie komendy, która umożliwi: a. usunięcie zawartości urządzenia b. zablokowania urządzenia c. przesłania na zaufany numer telefonu lokalizacji GPS, w której skradzione urządzenie się znajduje; • Administrator musi mieć możliwość wysyłania powyższych komend bezpośrednio z poziomu konsoli centralnego zarządzania.	**Wymagane**
75	**Posiadać funkcję polityki ustawień:** • Aplikacja musi posiadać funkcjonalność pozwalającą administratorowi na monitorowanie ustawień urządzenia w celu weryfikacji, czy są one zgodne z polityką; • Administrator musi mieć wgląd w podstawowe ustawienia urządzenia; • Administrator ma mieć możliwość wyboru powyższych elementów.	**Wymagane**

76	**Umożliwiać kontrolę aplikacji:** • Rozwiązanie musi umożliwiać administratorowi podejrzenie listy zainstalowanych aplikacji; • Administrator musi mieć możliwość blokowania zdefiniowanych aplikacji i poprosić użytkownika o odinstalowanie blokowanej aplikacji; • Blokowanie aplikacji musi być umożliwione co najmniej za pomocą polityk: a. manualnego zdefiniowania listy blokowanych aplikacji na podstawie nazwy b. blokowanie na podstawie kategorii c. blokowanie na podstawie uprawnień aplikacji d. blokowanie na podstawie źródła instalacji.	**Wymagane**
77	**Aktualizować sygnatury:** • Wymuszenie pobrania aktualizacji na żądanie ma być dostępne z poziomu interfejsu aplikacji; • Aplikacja ma mieć możliwość określenia harmonogramu zgodnie, z którym pobierane będą aktualizacje sygnatur.	**Wymagane**
78	**Umożliwiać konfigurację i zdalne zarządzanie:** • Administrator musi mieć możliwość eksportu/importu ustawień z/do pliku w celu przeniesienia konfiguracji na inne urządzenie mobilne; • Administrator musi mieć możliwość zabezpieczenia ustawień aplikacji hasłem przed ich modyfikacją; • Administrator musi mieć możliwość kontrolowania mechanizmu aktualizacji oprogramowania.	**Wymagane**

Wymagania systemowe:		
79	Pełne wsparcie dla systemów MS Windows 7 / 8 / 10.	**Wymagane**
80	Wykorzystywanie wcześniejszych wersji oprogramowania w trybie *downgrade* dla starszych systemów operacyjnych.	**Wymagane**
81	Wsparcie dla 32-bitowej i 64-bitowej wersji systemu MS Windows	**Wymagane**
82	Wersja programu dla stacji roboczych MS Windows musi być dostępna zarówno w języku polskim, jak i angielskim.	**Wymagane**
83	Pomoc w programie (ang. *help*) i dokumentacja do programu dostępne w języku polskim.	**Wymagane**

Należy podać:

- Cenę netto w PLN / brutto w PLN (cena winna obejmować koszty opakowania, transportu i ubezpieczenia od Wykonawcy do Zamawiającego) oraz stawkę i wartość podatku VAT,
- Warunki gwarancji
- Termin dostawy i warunki wykonania zamówienia,
- Warunki płatności.

Miejsce i termin składania ofert

Wstępną ofertę należy złożyć do dnia 08/11/2018 r. drogą elektroniczną, lub w siedzibie Zamawiającego:

Główny Instytut Górnictwa
Plac Gwarków 1, 40-166 Katowice
adres e-mail: makolczyk@gig.eu

mgr Monika Wallenburg - tel. (32) 259 25 47- e-mail: **mwallenburg@gig.eu**

mgr inż. Marzena Kolczyk - tel. (32) 259 23 42- e-mail: **makolczyk@gig.eu**

ZAPRASZAMY DO SKŁADANIA OFERT

Kierownik Działu Kadrowego
Głównego Instytutu Górnictwa
mgr Monika Wallenburg