Ministerstwo
Edukacji i Nauki

Biuro Dyrektora Generalnego

BDG-WII.072.4.2023

Warszawa, dnia 23 maja 2023 r.

Wykonawcy

ZAPYTANIE O WYCENĘ

Ministerstwo Edukacji i Nauki (MEiN), ul. Wspólna 1/3, 00-529 Warszawa (NIP 7011010460, REGON 387796051) zwraca się z prośbą o przedstawienie propozycji cenowej (oszacowanie wartości zamówienia) dotyczącej **wykonania modernizacji systemu zabezpieczeń brzegowych i rozbudowa ochrony serwerów i stacji roboczych**.

Opis przedmiotu zamówienia został określony w *Załączniku nr 1* do zapytania o wycenę.

Wycenę, sporządzoną na Formularzu będącym *Załącznikiem nr 2* do zapytania o wycenę, proszę przesłać na adres oferty@mein.gov.pl **do dnia 31 maja 2023 r., godz. 12:00** (w tytule wiadomości proszę wpisać: „WYCENA – sprawa: BDG-WII.072.4.2023)".

Ewentualne pytania mające wpływ na przedmiotową wycenę proszę kierować na adres mailowy jak wyżej.

Załączniki:

1) Opis przedmiotu zamówienia
2) Formularz wyceny

Łukasz Tererycz
Zastępca Dyrektora
/ – podpisano cyfrowo/

tel. (22) 52 92 725, (22) 34 74 157
sekretariat.bdg@mein.gov.pl, sekretariat.bdg.edukacja@mein.gov.pl
www.mein.gov.pl

ul. Wspólna 1/3
00-529 Warszawa

Załącznik nr 1 do zapytania o wycenę

OPIS PRZEDMIOTU ZAMMÓWIENIA

Modernizacja systemu zabezpieczeń brzegowych i rozbudowa ochrony serwerów i stacji roboczych

I. Przedmiot zamówienia

Zamawiający posiada system zabezpieczeń typu Next Generation Firewall z funkcją Sandbox firmy Checkpoint. Przedmiotem zamówienia jest:

a) modernizacja Systemu Zabezpieczeń Brzegowych typu Next Generation Firewall z funkcją Sandbox,
b) rozbudowa systemu o system typu Endpoint protection,
c) usługi wdrożenia,
d) usługa wsparcia technicznego producenta dla dostarczonego systemu (w tym do dostarczonych licencji) na okres 36 miesięcy,
e) usługa utrzymania i wsparcia serwisowego Wykonawcy na okres 36 miesięcy,
f) przeprowadzenie autoryzowanych szkoleń z dostarczonych rozwiązań.

II. Wymagania dotyczące modernizacji Systemu – dwa urządzenia typu Firewall

Modernizacja rozwiązania typu Next Generation Firewall z funkcją Sandbox wraz z dedykowanym oprogramowaniem i licencjami pozwalającymi na ich użytkowanie w środowisku Zamawiającego, na które składają się:

a) modernizacja dwóch urządzeń typu Firewall (1 klaster urządzeń),
b) integracja z posiadanym przez zamawiającego systemem zarządzania i systemem typu Sandbox,
c) usługa wdrożenia (instalacja i konfiguracja) i instruktażu,
d) przedłużenie wsparcia producenta na funkcjonalności: system zarządzania, system Sandbox, aktualizację bazy ataków IPS, definicji aplikacji, definicji wirusów oraz bazy kategorii stron WWW na okres 36 miesięcy.

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Dostarczone urządzenia zabezpieczeń sieciowych dostarczone będą w obudowie typu rack.
2.	Urządzenia oraz dedykowane do nich oprogramowanie i licencje muszą pochodzić od tego samego producenta (urządzenia typu appliance).
3.	Minimalna liczba i rodzaj portów - 8 portów 1000 BaseT, 8 portów 10 Gigabit SFP+.
4.	Musi posiadać możliwość przebudowy (tzn. wymiany interfejsów) dla wszystkich slotów.
5.	Firewall musi być wyposażony w 4 moduły SFP+ 10Gb-SR pochodzące od tego samego producenta co Firewall.
6.	Minimum 2 dyski SSD o pojemności nie mniejszej niż 460 GB w konfiguracji RAID 1.
7.	Minimum 2 redundantne zasilacze AC.
8.	Pamięć RAM minimum 64 GB.
9.	Dedykowany port do zarządzania out-of-band 1000 BaseT.
10.	Przepustowość ruchu nie mniej niż 22 Gbps dla kontroli NGFW (Firewall, Application Control, IPS) - dla ruchu typu Enterprise.
11.	Przepustowość ruchu nie mniejszą niż 9,4 Gbps z włączonymi wszystkimi elementami ochrony NGFW, Threat Prevention + Sandbox - dla ruchu typu Enterprise.
12.	Wydajność przynajmniej 11,8 Gbps dla ruchu VPN (przynajmniej AES-128).
13.	Przepustowość ruchu nie mniejsza niż 76 Gbps dla kontroli Firewall (pakiety 1518B UDP).
14.	Obsługa minimum 328 000 nowych połączeń na sekundę.
15.	Obsługa minimum 16 000 000 jednoczesnych połączeń.
16.	Obsługa minimum 4 000 tuneli IPsec.
17.	Obsługa minimum 3 000 polityk/reguł Firewall.
18.	Obsługa wirtualnych Firewalli z możliwością rozbudowy do minimum 20 wirtualnych Firewalli.
19.	Rozwiązanie musi umożliwić podłączenie urządzeń Firewall w klastrze pod scentralizowany system zarządzania i Sandbox posiadane przez Zamawiającego.
20.	Zapewniona obsługa dla IPv6.

21.	System zabezpieczeń Firewall musi działać zgodnie z zasadą bezpieczeństwa „The Principle of Least Privilege", tzn. system zabezpieczeń blokuje wszystkie aplikacje, poza tymi, które w regułach polityki bezpieczeństwa Firewall są wskazane jako dozwolone.
22.	Definiowanie własnych wzorców aplikacji poprzez zaimplementowane mechanizmy lub z wykorzystaniem serwisu producenta.
23.	Polityka zabezpieczeń Firewall uwzględnia adresy IP klientów i serwerów, protokoły i usługi sieciowe, aplikacje, użytkowników aplikacji oraz umożliwia rejestrowanie zdarzeń i alarmowanie.
24.	Statyczna i dynamiczna translacja adresów NAT. Mechanizmy NAT muszą umożliwiać, co najmniej dostęp wielu komputerów posiadających adresy prywatne do Internetu z wykorzystaniem jednego publicznego adresu IP oraz udostępnianie usług serwerów o adresacji prywatnej w sieci Internet.
25.	Statyczna i dynamiczna translacja adresów NAT między IPv4 i IPv6.
26.	Obsługa protokołu Ethernet z obsługą sieci VLAN poprzez tagowanie zgodne z IEEE 802.1q.
27.	Tworzenie subinterfejsów VLAN, które to mogą być kreowane na interfejsach sieciowych pracujących zarówno w trybie L2 jak i L3.
28.	Działanie urządzenia w trybie routera (tzn. w warstwie 3 modelu OSI), w trybie transparentnym (tzn. w warstwie 2 modelu OSI). Funkcjonując w trybie transparentnym urządzenie nie może posiadać skonfigurowanych adresów IP na interfejsach sieciowych.
29.	Tryb pracy urządzenia ma być ustalany na poziomie konfiguracji interfejsu sieciowego. System umożliwia pracę we wszystkich dostępnych trybach (router, transparentny) na różnych interfejsach inspekcyjnych w pojedynczej logicznej instancji systemu (np. wirtualny system, wirtualna domena, itp.).
30.	Obsługa protokołów routingu dynamicznego, przynajmniej BGP, RIP i OSPF.
31.	System zabezpieczeń Firewall musi być produktem o uznanej marce na rynku bezpieczeństwa IT. Potwierdzeniem tego faktu musi być obecność danego producenta systemu zabezpieczeń w raportach Gartner Magic Quadrant for Enterprise Network Firewalls w kwadracie liderów (Leaders) przez co najmniej 3 (trzy) ostatnie lata z rzędu.
32.	Zarządzanie pasmem sieci (QoS) w zakresie oznaczania pakietów znacznikami DiffServ, a także ustawiania dla dowolnych usług priorytetu, pasma maksymalnego i gwarantowanego.
33.	Możliwość integracji ze środowiskiem wirtualnym VMware w taki sposób, aby Firewall mógł automatycznie pobierać informacje o uruchomionych maszynach wirtualnych (np. ich nazwy) i korzystał z tych informacji do budowy polityk bezpieczeństwa. Tak zbudowane polityki powinny skutecznie klasyfikować i kontrolować ruch bez względu na rzeczywiste adresy IP maszyn wirtualnych i jakakolwiek zmiana tych adresów nie powinna pociągać za sobą konieczności zmiany konfiguracji polityk bezpieczeństwa Firewalla.
34.	Posiadanie funkcji ochrony przed atakami typu DoS wraz z możliwością limitowania ilości jednoczesnych sesji w odniesieniu do źródłowego lub docelowego adresu IP.
35.	Umożliwienie realizacji zadań kontroli dostępu (filtracji ruchu sieciowego), poprzez kontrolę ruchu na poziomie warstw sieciowej, transportowej oraz aplikacji.
36.	Możliwość pracy w konfiguracji odpornej na awarie w trybie klastra Active-Passive i Active-Active.
37.	W trybie Active-Active oba urządzenia powinny przyjmować bezpośrednio ruch sieciowy, przetwarzać go oraz analizować pod kątem bezpieczeństwa, tak aby rozkład obciążenia był jak najbardziej równomierny.
38.	Zestawianie i obsługa zabezpieczonych kryptograficznie tuneli VPN w oparciu o standardy IPSec i IKE w konfiguracji site-to-site. Dostęp VPN dla użytkowników mobilnych musi odbywać się na bazie technologii SSL VPN Portal oraz tunelu VPN (Layer-3 VPN Tunnel).
39.	Urządzenia powinny pozwalać na nielimitowany dostęp dla użytkowników mobilnych. Minimalne wsparcie dla systemów operacyjnych to Windows, Android, iOS.
40.	Możliwość uruchomienia modułu filtrowania stron WWW per reguła polityki bezpieczeństwa Firewall. Nie jest dopuszczalne, aby funkcjonalność filtrowania stron WWW uruchamiana była per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
41.	Możliwość ręcznego tworzenia własnych kategorii filtrowania stron WWW i używania ich w politykach bezpieczeństwa bez użycia zewnętrznych narzędzi i wsparcia producenta.

42.	Posiadanie modułu inspekcji antywirusowej dla protokołów: http, smtp, smb, pop3, imap bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur antywirus musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
43.	Możliwość uruchomienia modułu inspekcji antywirusowej per reguły polityki bezpieczeństwa pozwalającej na definiowanie co najmniej adresu źródłowego, docelowego oraz serwisu. Nie jest dopuszczalne, aby moduł inspekcji antywirusowej uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
44.	Posiadanie modułu umożliwiającego wykrywanie i blokowanie ataków intruzów w warstwie 7 modelu OSI IPS/IDS bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur IPS/IDS musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
45.	Możliwość uruchomienia wykrywania i blokowania ataków per reguły polityki bezpieczeństwa pozwalającego na definiowanie co najmniej adresu źródłowego, docelowe oraz serwisu. Nie jest dopuszczalne, aby moduł anty-spyware uruchamiany był per urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
46.	Posiadanie modułu chroniącego przed wirusami, złośliwym i szpiegowskim oprogramowaniem (moduł anty-malware) bez konieczności dokupowania jakichkolwiek komponentów, poza subskrypcją. Baza sygnatur anty-malware musi być przechowywana na urządzeniu, regularnie aktualizowana w sposób automatyczny i pochodzić od tego samego producenta co producent systemu zabezpieczeń.
47.	Możliwość uruchomienia modułu inspekcji anty-malware per reguły polityki bezpieczeństwa pozwalającej na definiowanie co najmniej adresu źródłowego, docelowego oraz serwisu. Nie jest dopuszczalne, aby moduł anty-spyware uruchamiany był przez urządzenie lub jego część (np. interfejs sieciowy, strefa bezpieczeństwa).
48.	Posiadanie sygnatur DNS wykrywających i blokujących ruch do domen uznanych za złośliwe.
49.	Funkcjonalność podmiany adresów IP w odpowiedziach DNS dla domen uznanych za złośliwe w celu łatwej identyfikacji stacji końcowych pracujących w sieci LAN zarażonych złośliwym oprogramowaniem (tzw. DNS Sinkhole).
50.	Posiadanie funkcji wykrywania aktywności sieci typu Botnet na podstawie analizy behawioralnej.
51.	Możliwość identyfikacji co najmniej 2500 różnych aplikacji, w tym aplikacji tunelowanych w protokołach HTTP i HTTPS m.in.: Skype, Gadu-Gadu, Tor, BitTorrent, eMule.
52.	Możliwość automatycznej identyfikacji aplikacji bez względu na numery portów, protokoły tunelowania i szyfrowania (włącznie z P2P i IM).
53.	Identyfikacja aplikacji musi odbywać się co najmniej poprzez sygnatury i analizę heurystyczną.
54.	Nie jest dopuszczalne, aby blokownie aplikacji (P2P, IM, itp.) odbywało się poprzez inne mechanizmy ochrony niż Firewall.
55.	Możliwość blokowania wysyłania i ściągania konkretnych typów plików.
56.	Możliwość skanowania całości ruchu pod kątem zaistnienia ataku, a nie wyłącznie wybranych próbek ruchu.
57.	Zapewnienie inspekcji komunikacji szyfrowanej dla protokołu HTTPS (HTTP szyfrowane protokołem TLS/SSL) dla ruchu wychodzącego do serwerów zewnętrznych (np. komunikacji użytkowników surfujących w Internecie). System musi posiadać możliwość deszyfracji niezaufanego ruchu HTTPS i poddania go właściwej inspekcji nie mniej niż: wykrywanie i blokowanie ataków typu exploit (ochrona Intrusion Prevention), wirusy i inny złośliwy kod (ochrona anty-malware), filtracja plików, URL i Sandbox.
58.	Możliwość transparentnego ustalania tożsamości użytkowników sieci w oparciu o Active Directory oraz CISCO ISE. Polityka kontroli dostępu (firewall) musi precyzyjnie definiować prawa dostępu użytkowników do określonych usług w sieci i musi być utrzymana nawet, gdy użytkownik zmieni lokalizację i adres IP. W przypadku użytkowników pracujących w środowisku terminalowym, tym samym mających wspólny adres IP, ustalanie tożsamości musi odbywać się również transparentnie.

59.	W przypadku transparentnego ustalania tożsamości użytkowników sieci w oparciu o Active Directory nie jest wymagana instalacja dodatkowych komponentów (np. dodatkowego oprogramowania lub urządzenia).
60.	Urządzenie umożliwia czytanie oryginalnych adresów IP stacji końcowych z nagłówka XForwarded-For i wykrywania na tej podstawie użytkowników generujących daną sesje, w przypadku gdy ruch przechodzi przez serwer Proxy zanim dojdzie do urządzenia.
61.	Urządzenie nie może posiadać ograniczeń licencyjnych dotyczących liczby chronionych komputerów w sieci wewnętrznej.
62.	Dostęp do urządzenia i zarządzanie z sieci muszą być zabezpieczone kryptograficznie (poprzez szyfrowanie komunikacji).
63.	Interfejs administracyjny urządzenia musi być w języku polskim lub angielskim.
64.	Możliwość uwierzytelniania administratorów za pomocą bazy lokalnej, serwera RADIUS lub TACACS+.

III. <u>Wymagania minimalne dotyczące urządzenia typu Endpoint protection</u>

Na potrzeby rozwiązania XDR wykonawca dostarczy dedykowane rozwiązanie oraz system zarządzający wraz z licencjami oprogramowania pozwalającymi na jego użytkowanie w środowisku Zamawiającego.

Wymagane ilości oraz typy urządzeń:

- Desktop, serwer, laptopy: 750
- Urządzenia mobile: 250

1. System centralnego zarządzania

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Rozwiązanie musi posiadać konsole centralnego zarządzania dostępną jako maszyna wirtualna.
2.	Serwer centralnego zarządzania musi obsługiwać do 400 000 tysięcy punktów końcowych.
3.	Serwer centralnego zarządzania musi posiadać działający i bardzo dobrze udokumentowany interfejs API.
4.	Serwer centralnego zarządzania musi umożliwiać tworzenie reguł dla klientów końcowych, oparty na politykach zarządzających.
5.	Serwer centralnego zarządzania musi pozwalać na tworzenie odrębnego zestawu polityk dla komputerów podłączonych do serwera centralnego zarządzania, oraz tych będących offline i niepodłączonych do serwera centralnego zarządzania.
6.	Serwer centralnego zarządzania oparty o chmurę, musi posiadać mechanizm EDR pozwalający na wyszukiwanie i "polowanie" na zagrożenia sieciowe posiadający co najmniej 130 różnych znaczników, z których można budować wyszukiwania.
7.	Serwer centralne zarządzania musi pozwalać na tworzenie dostępów administracyjnych opartych o role.
8.	Serwer centralnego zarządzania musi mieć możliwość definiowania wykluczeń m.in. w zakresie: a. Kontroli filtrowania stron WWW, b. Ochrony antywirusowej w czasie rzeczywistym, c. Skanowania na żądanie, d. Konkretnych nazw ataków, e. Modułów emulacyjnych zagrożenia, f. Ochrony behawioralnej, g. Lista wykluczeń musi być dostępna dla każdej z wyżej wymienionych kategorii z osobna.

9.	Serwer centralnego zarządzania musi umożliwiać wysyłanie minimum następujących zadań do klienta antywirusowego: a. Skanowanie komputera, b. Aktualizacja sygnatur antywirusowych, c. Przywracania plików z kwarantanny, d. Analizy konkretnego procesu działającego na systemie operacyjnym, e. Przeniesienia, lub usunięcia pliku do/z kwarantanny, f. Izolacji komputera, usunięcia komputera z izolacji, g. Wypchnięcia nowego klienta antywirusowego, h. Zebrania logów z klienta, i. Naprawy instalacji klienta antywirusowego, j. Wyłączenia komputera, k. Odinstalowania klienta antywirusowego, l. Skanowania konkretnej aplikacji, m. Zabicia konkretnego procesu pracującego w systemie operacyjnym, n. Wywołania skryptu PowerShell.
10.	Serwer centralnego zarządzania musi posiadać funkcjonalność logowania zdarzeń ze stacji końcowych.
11.	Serwer centralnego zarządzania musi posiadać funkcjonalność raportowania zdarzeń w formie graficznej.
12.	Serwer centralnego zarządzani musi umożliwiać zarządzanie wieloma organizacjami z poziomu jednej konsoli centralnego zarządzania.

2. Klient endpoint

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Wsparcie systemów Windows: Windows 10, Windows 11, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022.
2.	Wsparcie systemów Linux: Ubuntu, Debian, RHEL, CentOS, Oracle Linux, Amazon Linux.
3.	Wsparcie systemów macOS: 10.14, 10.15, 11.
4.	Klient antywirusowy musi wspierać systemy pracujące w środowisku zwirtualizowanym.
5.	Wsparcie dla rozwiązań VDI.
6.	Plik instalacyjny programu musi być mniejszy niż 1 MB.
7.	Plik instalacyjny musi być dostępny zarówno jako plik z rozszerzeniem *.exe jak i *.msi.
8.	Plik instalacyjny musi umożliwiać prostą instalację w środowisku rozproszonym wykorzystując skrypty instalacyjne czy pozwalając na instalację z poziomu GPO i SCCM.
9.	Rozwiązanie musi posiadać własny system dystrybucji nowych paczek instalacyjnych w środowisku rozproszonym, który nie wykorzystuje technologii zewnętrznych takich jak np. Microsoft SCCM czy Intune.
10.	Klient antywirusowy musi posiadać następujące moduły bezpieczeństwa: a. Antymalware, b. URL Filtering, c. Moduł analizy behawioralnej, d. Moduł blokowania dostępu do urządzeń podłączanych do komputera, e. Firewall i kontrola aplikacji, f. Moduł weryfikacji zgodności, g. Moduł emulacji zagrożeń, h. Funkcja pełnego szyfrowania dysku musi wykorzystywać instrukcje procesora AES-NI w celu optymalizacji procesu szyfrowania.
11.	Klient antywirusowy musi posiadać moduł anty-ransomware umożliwiający wykrycie, zablokowanie infekcji i przywrócenie zaszyfrowanych plików.
12.	Klient antywirusowy musi posiadać moduł ochrony przed wirusami bezplikowymi.
13.	Klient antywirusowy musi być zintegrowany z interfejsem Microsoft Anti-Malware Scan Interface (AMSI) w celu odbierania i analizowania zdekodowanych skryptów.
14.	Klient antywirusowy musi posiadać moduł wykrywający komunikację do serwerów C&C, oraz umożliwiać jej blokowanie.
15.	Rozwiązanie w ramach podstawowej licencji musi umożliwiać aktualizacje baz serwerów C&C i ataków typu zero-day w czasie rzeczywistym, bezpośrednio z chmury producenta.

16.	Klient antywirusowy musi mieć możliwość instalacji modułowej tj. pozwolić na instalację każdego z dostępnych modułów z osobna.
17.	Klient antywirusowy musi umożliwiać ukrycie ikony programu na tacce systemowej.
18.	Klient antywirusowy musi umożliwiać na zezwolenie, lub zablokowanie możliwości przeglądania logów programu przez użytkownika komputera.
19.	Klient antywirusowy musi umożliwiać definiowanie jakie typy komunikatów będą wyświetlane użytkownikowi przynajmniej na 3 poziomach.
20.	Klient antywirusowy musi umożliwiać na wgranie pliku graficznego z logo firmy, które będzie wykorzystywane w komunikatach programu antywirusowego, wyświetlanych użytkownikowi.
21.	Klient antywirusowy musi umożliwiać konfiguracje tła logowania w systemie Windows, na zdefiniowane przez administratora.
22.	Klient antywirusowy musi umożliwiać zabezpieczenie odinstalowania programu poprzez zdefiniowanie hasła wymagane do odinstalowania programu.
23.	Klient antywirusowy musi dawać możliwość wykorzystania jednego z 3 silników antywirusowych, z czego 2 muszą pochodzić od innego producenta, niż oferowane rozwiązanie.
24.	Klient antywirusowy musi mieć możliwość wykorzystania sandboxa lokalnego obsługiwanego przez dedykowany appliance sprzętowy posiadanego przez Zamawiającego.
25.	Klient antywirusowy musi generować raport z każdej wykrytej infekcji zawierający minimum: a. Informacje na temat źródła ataku, b. Pliki jakie zostały zaatakowane przez wirusa, c. Adresy sieciowe do jakich niebezpieczny proces próbował się połączyć, d. Informacje na temat wyleczenia lub usunięcia wirusa, e. Mapowanie wykrytych metod ataku na matrycę MITRE ATT&CK, f. Raport będzie rejestrował, prezentował i usuwał zaciemnienia skryptów PowerShell używanych podczas ataku, g. Raport z ataku musi być dostępny z poziomu logów, jak i możliwy do pobrania na komputer z konsoli administracyjnej.
26.	Klient antywirusowy musi posiadać plugin do przeglądarki internetowej umożliwiający skanowanie w czasie rzeczywistym ruchu WWW przynajmniej dla przeglądarek: a. Chrome, b. Firefox, c. Edge (Chromium).
27.	Rozwiązanie antywirusowe musi mapować wykryte ataki wirusów na matrycę MITRE ATT&CK z wykorzystaniem minimum 44 technik.
28.	Klient antywirusowy musi posiadać możliwość kontroli dostępu do portów USB.
29.	Klient antywirusowy musi posiadać możliwość blokowania zainstalowanych aplikacji na komputerze.
30.	Klient antywirusowy musi posiadać funkcjonalność weryfikowania zgodności z polityką firmy gdzie sprawdzane i raportowane do konsoli może być m.in. a. Aktualizacje systemu Windows Update i ostatnia zainstalowana aktualizacja systemu operacyjnego, b. Status wygaszacza ekranu wraz z włączoną opcją wymagania hasła po jego wyłączeniu, c. Weryfikacja dowolnych wartości kluczy rejestru.
31.	Klient antywirusowy musi być zdolny do zmiany ustawień wbudowanego firewalla, zależnie od statusu zgodności komputera, weryfikowanego przez moduł zgodności.
32.	Możliwość blokowania urządzeń podłączanych przez port USB do komputera.
33.	Automatyczne logowanie wszystkich urządzeń USB podpiętych do komputera chronionego przez rozwiązanie.
34.	Ochrona developerska zapobiegająca wyciekowi kluczy RSA, haseł, tokenów, przy wykorzystaniu Git'a.
35.	Klient antywirusowy musi posiadać technologię usuwania niebezpiecznej zawartości (makra, składniki aktywne, adresy URL) plików ściąganych z Internetu i dostarczania ich przed detonacją oryginalnego pliku w sanboxie.

3. Wymagania do całego systemy Endpoint

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Proponowane rozwiązanie musi posiadać możliwość integracji z rozwiązaniem do orkiestracji danych.
2.	Rozwiązanie musi być zgodne z ustawą o zarządzaniu bezpieczeństwem informacji (FISMA).
3.	Rozwiązanie musi spełniać ramy zarządzania ryzykiem DoD (RMF).
4.	Rozwiązanie musi spełniać standardy bezpieczeństwa branży kart płatniczych (PCI).

IV. Pozostałe wymagania dla dostarczanego rozwiązania

Lp.	MINIMALNE WYMAGANIA ZAMAWIAJĄCEGO
1.	Wszystkie dostarczone urządzenia wraz z wymaganymi licencjami oprogramowania muszą być objęte wsparciem technicznym producenta świadczonym w okresie 36 miesięcy od daty wdrożenia Systemu. Dla potwierdzenia objęcia ww. wsparciem urządzeń dostarczonych Zamawiającemu, Wykonawca dostarczy wraz z urządzeniem i oprogramowaniem dokument potwierdzający nabycie praw przez Zamawiającego do wsparcia producenta.
2.	Wsparcie powinno być świadczone telefonicznie oraz pocztą elektroniczną przez producenta lub jego autoryzowanego polskiego przedstawiciela serwisowego. Powinno obejmować co najmniej wymianę uszkodzonego sprzętu, dostęp do nowych wersji oprogramowania, a także dostęp do baz wiedzy, przewodników konfiguracyjnych i narzędzi diagnostycznych.
3.	W ramach zamówienia wykonawca musi dostarczyć przedłużenie subskrypcji i wsparcie producenta dla licencji na funkcjonalności: Management wraz z SmartEvent, AntiSPAM i E-mail Security, Sandbox, Application Control, na aktualizację bazy ataków IPS, definicji aplikacji, definicji wirusów oraz bazy kategorii stron WWW na okres 36 miesięcy.
4.	Wymagane jest, aby dostarczone Urządzenia były sprzętem zakupionym w oficjalnym kanale sprzedaży producenta na terenie Unii Europejskiej. Zamawiający zastrzega możliwość weryfikacji powyższego wymogu u przedstawiciela producenta oferowanego rozwiązania (np. przez weryfikację telefoniczną u producenta nr seryjnych podanych przez wykonawcę).
5.	Wymagane jest, aby Urządzenia były fabrycznie nowe (nieużywane, nieregenerowane, niefabrykowane) wolne od wad, przeznaczone do sprzedaży na rynku europejskim (zgodnie z ustawą z dnia 30.08.2002 r. o systemie oceny zgodności (Dz. U. z 2019 r., poz. 155) i z wydanymi na jej podstawie rozporządzeniami, wyprodukowane nie wcześniej niż 6 miesięcy przed datą dostarczenia oraz objęte wymaganą przez zamawiającego gwarancją w Polsce.
6.	Wymagane jest, aby Urządzenia nie były produktem „odnawialnym" (ang. Refurbished) oraz na dzień składania ofert nie były przeznaczone przez producenta do wycofania z produkcji lub sprzedaży.
7.	Dostarczone urządzenia muszą pochodzić z legalnego źródła, być zakupione w autoryzowanym kanale sprzedaży producenta w Polsce i objęte gwarancją na okres 36 miesięcy licząc od dnia podpisania Protokołu Odbioru , świadczonej poprzez sieć serwisową producenta na terenie Polski.

V. Wdrożenie

1. Modernizacja i konfiguracja nowo dostarczonych urządzeń.
2. Wdrożenie i konfiguracja systemu XDR.
3. Konfiguracja bazowych polityk dla systemu XDR (zgodne z best practice).
4. Pilotażowa instalacja (dostarczenie ew. skryptów) na 10 urządzeniach Zamawiającego.

VI. Szkolenia

1. Przeprowadzenie 6 autoryzowanych szkoleń z administrowania zaoferowanym rozwiązaniem.
2. Plan szkoleń będzie uzgodniony na etapie wdrożenia.
3. Szkolenie musi odbyć się na terytorium Polski w mieście siedziby Zamawiającego.
4. Jeden ciepły posiłek.

5. Czas pojedynczego szkolenia min. 2 dni.
6. Szkolenia będą zrealizowane w przeciągu 12 miesięcy.
7. Zamawiający zastrzega sobie możliwość 6 szkoleń o różnym programie w różnych terminach.

VII. <u>Wsparcie techniczne wykonawcy na 36 miesięcy</u>

Wykonawca musi zapewnić poniższy zakres usług realizowanych przez specjalistów posiadających aktualne certyfikaty:

1) Utrzymanie środowiska (System Firewall i XDR)

a) zapewnienie SLA dla całego Systemu Firewall:
– czas reakcji: 4h
– czas usunięcia awarii lub znalezienia obejścia: 1 dzień roboczy,
b) aktualizacje/patchowanie Systemu Firewall i XDR: nie rzadziej niż 2 razy do roku,
c) audyt Best Practices Assessment: nie rzadziej niż 1 w roku,
d) aktywny monitoring elementów tworzących System Firewall i XDR,
e) bieżące reagowanie na błędy / awarie,
f) eskalacja problemów technicznych / błędów w oprogramowaniu do producenta,
g) wykonywanie podstawowych procedur utrzymaniowych (zarządzanie
h) pojemnością, monitorowanie parametrów usług, nadzór nad procesem
i) archiwizacji, monitorowanie licencji, itp.);

2) Usługi rozwojowe dla Systemu Firewall i XDR:

a) informowanie o nowych funkcjach i podatnościach,
b) proponowanie zmian w konfiguracji pod kątem zwiększenia bezpieczeństwa systemu,
c) wdrażanie zaleceń audytu Best Practices Assessment.

Załącznik nr 2 do zapytania o wycenę
FORMULARZ WYCENY

Wykonawca (pełna nazwa albo imię i nazwisko)		
Siedziba/miejsce zamieszkania i adres jeżeli jest miejscem wykonywania działalności Wykonawcy		
numer KRS (w zależności od podmiotu)		
Imię nazwisko, stanowisko/podstawa **do reprezentacji**		
NIP/REGON		
telefon		
e-mail		
Osoba do kontaktów z Zamawiającym		
Czy Wykonawca jest mikroprzedsiębiorstwem bądź małym lub średnim przedsiębiorstwem[1]?	[ ] Tak / [ ] Nie	Mikroprzedsiębiorstwo
	[ ] Tak / [ ] Nie	Małe przedsiębiorstwo
	[ ] Tak / [ ] Nie	Średnie przedsiębiorstwo

W przypadku składania oferty przez Wykonawców wspólnie ubiegających się o udzielenie zamówienia należy podać pełne nazwy i dokładne adresy wszystkich Wykonawców wspólnie ubiegających się o udzielenie zamówienia, a także wskazać Pełnomocnika)

Ministerstwo Edukacji i Nauki
ul. Wspólna 1/3
00-529 Warszawa

W odpowiedzi na zapytanie o wycenę za wykonanie modernizacji systemu zabezpieczeń brzegowych i rozbudowa ochrony serwerów i stacji roboczych (znak: BDG-WII.072.4.2023), przedstawiam wycenę jak niżej.

[1] **Por. *zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (Dz.U. L 124 z 20.5.2003, s. 36). Te informacje są wymagane wyłącznie do celów statystycznych. Mikroprzedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 10 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 2 milionów EUR. Małe przedsiębiorstwo: przedsiębiorstwo, które zatrudnia mniej niż 50 osób i którego roczny obrót lub roczna suma bilansowa nie przekracza 10 milionów EUR. Średnie przedsiębiorstwa: przedsiębiorstwa, które nie są mikroprzedsiębiorstwami ani małymi przedsiębiorstwami* i które zatrudniają mniej niż 250 osób i których roczny obrót nie przekracza 50 milionów EUR *lub* roczna suma bilansowa nie przekracza 43 milionów EUR.**

Lp.	*Nazwa*	*szt.*	*Cena jednostkowa brutto PLN*	*Wartość brutto PLN (kol. 3 x kol. 4)*
1	*2*	*3*	*4*	*5*
1	**Modernizacja rozwiązania typu Next Generation Firewall** *Model:* **……***(należy wpisać)* *Producent:* **……** *(należy wpisać)* *Nr produktu:* **……** *(należy wpisać)*	**2**	……	……
2	**Licencje XDR (**Desktop, serwer, laptopy) *Model:* **……***(należy wpisać)* *Producent:* **……** *(należy wpisać)* *Nr produktu:* **……** *(należy wpisać)*	**750**	……	……
3	**Licencje XDR (**Urządzenia mobile) *Model:* **……***(należy wpisać)* *Producent:* **……** *(należy wpisać)* *Nr produktu:* **……** *(należy wpisać)*	**250**	……	……
9	**Przedłużenie wsparcia i licencji dla posiadanych komponentów** Managment i Sandbox *Producent:* …… *(należy wpisać)* *Nr produktu:* …… *(należy wpisać)*			……
10	**Wsparcie i licencje dla zaoferowanych komponentów** *Producent:* …… *(należy wpisać)* *Nr produktu:* …… *(należy wpisać)*			……
11	**Wsparcie wykonawcy do dostarczone rozwiązanie**			……
12	**USŁUGA WDROŻENIA**			……
13	**Przeprowadzenie 6 autoryzowanych szkoleń**			……
	CENA CAŁKOWITA ZA REALIZACJĘ ZAMÓWIENIA (razem poz. 1-13)			**……**

data …… ……

podpis osoby/osób uprawnionej/uprawnionych do reprezentowania Wykonawcy

Informacja dla Wykonawcy: Formularz wyceny musi być podpisany przez osobę lub osoby uprawnione do reprezentowania Wykonawcy podpisem własnoręcznym - wówczas oferta składana jest w formie skanu lub podpisem w formie elektronicznej (kwalifikowany podpis elektroniczny).

Załącznik nr 3 do zapytania o wycenę

Wycena zamówienia publicznego pn. wykonanie modernizacji systemu zabezpieczeń brzegowych i rozbudowa ochrony serwerów i stacji roboczych (sprawa: BDG-WII.072.4.2023).

Klauzula informacyjna dot. przetwarzania danych osobowych przez Zamawiającego

Zgodnie z art. 13 ust. 1 i 2 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1 oraz Dz. Urz. UE L 127 z 23.05.2018, str. 2), dalej „RODO", informuję, że:

1) administratorem Pani/Pana danych osobowych jest Ministerstwo Edukacji i Nauki;
2) dane kontaktowe do inspektora ochrony danych w Ministerstwie Edukacji i Nauki: Ministerstwo Edukacji i Nauki, ul. Wspólna 1/3, 00-529 Warszawa, adres e-mail: inspektor@mein.gov.pl;
3) Pani/Pana dane osobowe przetwarzane będą na podstawie art. 6 ust. 1 lit. c RODO w celu związanym z przeprowadzeniem postępowania o udzielenie zamówienia publicznego jak również zawarcia umowy w sprawie zamówienia oraz jej realizacji, a także udokumentowania postępowania o udzielenie zamówienia i jego archiwizacji;
4) odbiorcami Pani/Pana danych osobowych będą osoby lub podmioty, którym dokumentacja postępowania zostanie udostępniona /osoby lub podmioty zapewniające obsługę informatyczną Ministerstwa Edukacji i Nauki / wszystkie osoby, które zapoznają się z informacjami zamieszczonymi na stronie internetowej MEiN;
5) Pani/Pana dane osobowe będą przechowywane do czasu ustania celu jakim jest przeprowadzenie postępowania o udzielenie zamówienia, zawarcie i wykonanie umowy, a następnie, jeśli chodzi o materiały archiwalne, zgodnie z Instrukcją Kancelaryjną Ministerstwa Edukacji i Nauki oraz przepisami o archiwizacji dokumentów – przez okres co najmniej 5 lat od dnia przekazania ich do archiwum Ministerstwa Edukacji i Nauki;
6) obowiązek podania przez Panią/Pana danych osobowych jest wymogiem związanym z udziałem w postępowaniu o udzielenie zamówienia publicznego;
7) w odniesieniu do Pani/Pana danych osobowych decyzje nie będą podejmowane w sposób zautomatyzowany, stosowanie do art. 22 RODO;
8) posiada Pani/Pan:
   - na podstawie art. 15 RODO prawo dostępu do danych osobowych Pani/Pana dotyczących,
   - na podstawie art. 16 RODO prawo do sprostowania lub uzupełnienia Pani/Pana danych osobowych,
   - na podstawie art. 18 RODO prawo żądania od administratora ograniczenia przetwarzania danych osobowych,
   - prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych, gdy uzna Pani/Pan, że przetwarzanie danych osobowych Pani/Pana dotyczących narusza przepisy RODO.