DOSTAWA I WDROŻENIE SYSTEMU KLASY ADVANCED THREAT PROTECTION (ATP)

ZAPYTANIE O INFORMACJĘ (RFI)

Czerwiec 2020 r.

SPIS TREŚCI

1. INFORMACJE PODSTAWOWE

1.1. WŁASNOŚĆ DOKUMENTU

Niniejszy dokument stanowi własność Energa Informatyka i Technologie Sp. z o.o. (dalej: EITE), która w zakresie tego zapytania reprezentuje Grupę Energa. Kopiowanie lub rozpowszechnianie tego dokumentu, w całości lub częściowo, w jakiejkolwiek formie, jest niedozwolone bez uprzedniej zgody.

Energa Informatyka i Technologie Sp. z o.o. ma prawo zażądać w dowolnym momencie zwrotu wszystkich kopii tego dokumentu.

1.2. INFORMACJE NA TEMAT GRUPY ENERGA

Grupa ENERGA jest jedną z czterech grup elektroenergetycznych w Polsce. Siedziba spółki zarządzającej – Energa SA znajduje się w Gdańsku. Podstawowa działalność spółek Grupy obejmuje dystrybucję, wytwarzanie oraz obrót energią elektryczną, cieplną i gazem. Jesteśmy jednym z trzech największych dostawców energii elektrycznej w Polsce. Zasilamy w energię elektryczną ponad 2,9 mln klientów indywidualnych i biznesowych. Eksploatujemy ponad 184 tys. km linii energetycznych.

Wizja Grupy ENERGA zakłada stworzenie zwartej, efektywnej i innowacyjnej Grupy Kapitałowej, która dzięki współdziałaniu i wzajemnemu wspieraniu się wszystkich podmiotów Grupy jest liderem w zakresie jakości usług i obsługi na polskim rynku mediów użytkowych, stale podnoszącym swoją efektywność.

2. OPIS PRZEDMIOTU ZAPYTANIA

W związku z prowadzoną analizą rynku wykonawców, zapraszamy Państwa do przedstawienia informacji obejmujących warunki kosztowe dla realizacji dostawy i wdrożenia systemu klasy Advanced Threat Protection (ATP) w Grupie Energa, wg wskazanych poniżej informacji.

Niniejszy dokument zawiera opis przedmiotu zapytania na „System klasy Advanced Threat Protection (ATP)". Celem dokumentu jest opisanie objętych zapytaniem licencji, komponentów i usług w ramach dostawy i wdrożenia systemu.

2.1. PRACE PRZEDWDROŻENIOWE

Wykonawca przeprowadzi niżej wymieniony zakres prac przedwdrożeniowych i na ich podstawie przygotuje dokumentację dla rozwiązania klasy Advanced Threat Protection (ATP):

1. analiza polityk retencji i wymaganej przestrzeni dyskowej,
2. zaprojektowanie docelowej architektury,

3. przygotowanie dokumentacji przedwdrożeniowej.

2.2. USŁUGA WDROŻENIA ŚRODOWISKA SYSTEMU KLASY ADVANCED THREAT PROTECTION (ATP)

Wykonawca przeprowadzi niżej wymieniony zakres prac wdrożeniowych:

1. wdrożenie systemu klasy Advanced Threat Protection (ATP) w zakresie ochrony 10700 urządzeń (stacji roboczych / serwerów),
2. integracja systemu ATP z rozwiązaniem klasy SIEM,
3. wdrożenie dwóch ośrodków (HA), o ile system umożliwia taką funkcjonalność,
4. konfiguracja automatycznych reakcji na wykryte zdarzenia, zróżnicowanych pod kątem poziomu zaistniałego naruszenia,
5. konfiguracja powiadomień o zdarzeniach, obejmujących możliwością informowania Zespołu Bezpieczeństwa,
6. konfiguracja 10 raportów, możliwych do uruchomienia ad-hoc jak i wykonywanych okresowo, o parametrach wskazanych przez Zamawiającego,
7. konfiguracja backupu wraz z testami odtworzeniowymi,
8. utworzenie dashboardów dla potrzeb SOC (Security Operations Center),
9. przygotowanie procedur Disaster Recovery dla środowiska ATP,
10. przygotowanie procedur eksploatacyjnych, obejmujących zarzadzanie rozwiązaniem, instalację agentów (lub proces objęcia osłoną stacji roboczych / serwerów dla rozwiązań bez agentowych),
11. przygotowanie dokumentacji powykonawczej.

2.3. USŁUGA BIEŻĄCEGO WSPARCIA

Wykonawca przez okres 36 miesięcy od momentu zakończenia prac wdrożeniowych i protokolarnego odbioru rozwiązania zapewnieni cykliczne wsparcie w konfiguracji i optymalizacji pracy systemu klasy Advanced Threat Protection (ATP) w wymiarze 8h miesięcznie z możliwością dynamicznego przesuwania godzin pomiędzy poszczególnymi miesiącami. Godziny niewykorzystane w danym miesiącu przechodzą na kolejne okresy rozliczeniowe. Godziny starsze niż 3 miesiące mogą zostać dostarczone przez Wykonawcę w terminie uzgodnionym przez strony, nie późniejszym jednak niż 1 miesiąc od złożenia zapotrzebowania.

2.4. SZKOLENIA

Wykonawca zapewni szkolenia zgodnie z poniższymi wymaganiami:

1. szkolenie dla analityków bezpieczeństwa z systemu klasy Advanced Threat Protection (ATP) – w wymiarze 24 godzin dla 10 osób (szkolenie w języku polskim, dokumentacja w języku angielskim lub polskim), zgodne ze ścieżką szkoleniową producenta,
2. szkolenie dla administratorów systemu klasy Advanced Threat Protection (ATP) – w wymiarze 40 godzin dla 4 osób (szkolenie w języku polskim, dokumentacja w języku angielskim lub polskim), zgodne ze ścieżką szkoleniową producenta.

2.5. ZAKUP LICENCJI

Wykonawca dostarczy Zamawiającemu licencje umożliwiające wdrożenie systemu klasy Advanced Threat Protection (ATP) zgodnie z poniższym:

1. Zamówienie podstawowe:
    a) objęcie osłoną systemem klasy Advanced Threat Protection 10700 stacji roboczych / serwerów wraz ze wsparciem producenta na okres 36 miesięcy,
    b) licencje dla wszystkich komponentów wymaganych do eksploatacji systemu klasy Advanced Threat Protection (ATP).
2. Zamówienie opcjonalne:
    a) licencje klienckie – urządzenia (pakiet 100),
    b) licencje klienckie – urządzenia (pakiet 500).

Zamawiający na etapie postępowania ofertowego zastrzeże sobie prawo możliwości zakupu tylko części licencji zawartych w zamówieniu opcjonalnym.

2.6. DODATKOWE INFORMACJE

1. Informacje umożliwiające opracowanie docelowej architektury systemu klasy Advanced Threat Protection (ATP) przez Wykonawcę zostaną udostępnione po podpisaniu odpowiednich dokumentów związanych z zachowaniem poufności.
2. Miejsce realizacji zamówienia: ENERGA Informatyka i Technologie, al. Grunwaldzka 472 A, 80-309 Gdańsk oraz al. Marszałka Piłsudskiego 41, 09-407 Płock.
3. Wykonawca zobowiązany jest do dostarczenia dokumentacji przedwdrożeniowej i na podstawie akceptacji Zamawiającego rozpocznie prace z niej wynikające. Dokumentacja przedwdrożeniowa powinna zawierać:
    a) docelową architekturę rozwiązania,
    b) parametry sprzętu koniecznego do zaimplementowania środowiska (serwery),

c) szczegółowy opis poszczególnych prac koniecznych (harmonogram wdrożenia) do wykonania w całym procesie wdrożeniowym wraz z uwzględnieniem sytuacji awaryjnych – możliwość powrotu do pierwotnej konfiguracji,

d) konfigurację docelowego rozwiązania obejmującą: uprawnienia zgodnie z przynależnością pracowników, sposób konfiguracji integracji.

4. Wykonawca zobowiązany jest przygotować dokumentację powdrożeniową, która musi zostać zaakceptowana przez Zamawiającego. Dokumentacja powdrożeniowa powinna zawierać:

a) architekturę wdrożonego systemu,

b) opis modułów wraz z adresacją IP oraz możliwościami dostępu,

c) opis ról i uprawnień wraz instrukcją modyfikowania uprawnień i dodawania nowych ról,

d) opis wszystkich prac wdrożeniowych wraz ze zrzutami ekranów,

e) opis wdrożonych scenariuszy bezpieczeństwa,

f) opis funkcjonowania środowiska redundantnego HA (High Availability) wraz z instrukcją przełączania pomiędzy środowiskiem podstawowym a redundantnym – uwzględnienie dobrych praktyk, o ile rozwiązanie klasy Advanced Threat Protection (ATP) dostarcza taką funkcjonalność,

g) opis parametrów wykorzystanego sprzętu,

h) opis sposobu aktualizacji systemu,

i) opis sposobu realizacji kopii bezpieczeństwa,

j) opis sposobu odtwarzania po awarii systemu na podstawie przygotowanych w trakcie prac wdrożeniowych kopii bezpieczeństwa,

k) opis konfiguracji i reguł zaimplementowanych podczas wdrożenia systemu,

l) opis wszelkich dodatkowych prac m.in. skrypty tworzone podczas wdrożenia.

3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP)

Zamawiający oczekuje dostarczenia rozwiązania, spełniającego poniższe wymagania:

Rozwiązanie musi spełniać następujące wymagania:

1. rozwiązanie musi być dostępne w modelu Licencja + wsparcie, w którym możliwe jest zakupienie trwałej licencji a następnie odnawianie co roku wsparcia technicznego lub w modelu licencji czasowych (1,2,3 lub więcej lat), których zakup (płatność) odbywa się jednorazowo, zawierających produkt, dostęp do aktualizacji oraz wsparcie.
2. rozwiązanie musi zapewniać możliwość integracji z wykorzystywanym oprogramowaniem antywirusowym na stacjach roboczych i serwerach,

3. rozwiązanie musi posiadać mechanizmy wykrywania zaawansowanych zagrożeń w kanale sieciowym,
4. rozwiązanie musi posiadać możliwość izolacji sieciowej (przełączenia do kwarantanny) hostów w przypadku detekcji na nich zagrożeń,
5. rozwiązanie musi posiadać mechanizmy wykrywania zaawansowanych zagrożeń na urządzeniu końcowym,
6. rozwiązanie musi posiadać możliwość poszukiwania urządzeń wykazujących się konkretnymi cechami (uruchomienie aplikacji, otwarcie konkretnego pliku),
7. rozwiązanie musi posiadać możliwość zdalnej remediacji zagrożenia, poprzez terminowanie procesów, usuwanie plików i zmian w rejestrach,
8. rozwiązanie musi prezentować zdarzenia w czasie rzeczywistym,
9. rozwiązanie musi być zarządzane z poziomu jednej konsoli,
10. rozwiązanie musi posiadać możliwość eksportu pozyskanych artefaktów do celów analitycznych i dowodowych,
11. rozwiązanie musi posiadać możliwość integracji z systemami klasy SIEM,
12. rozwiązanie musi wspierać osłonę systemów operacyjnych Microsoft w wersjach 32/64bit, wspieranych przez producenta, gdzie punktem odniesienia jest data 01.08.2019.
13. rozwiązanie musi wspierać starsze wersje systemów operacyjnych Microsoft w wersjach 32/64bit, od Windows 2003 R2 wzwyż dla platform serwerowych i Windows 7 dla stacji roboczych.
14. rozwiązanie powinno wspierać systemy operacyjne Linux,
15. rozwiązanie powinno umożliwiać budowę środowiska HA lub rozwiązanie musi zapewniać możliwość odtworzenia funkcjonalności po awarii oprogramowania w czasie nie dłuższym niż 4 godziny, bez utraty danych historycznych i raportowych,
16. rozwiązanie musi tworzyć incydenty z wykrytych zdarzeń,
17. rozwiązanie musi posiadać możliwość szczegółowego raportowania incydentów,
18. rozwiązanie musi posiadać możliwość raportowania, zarówno ad-hoc jak i cyklicznego,
19. rozwiązanie musi umożliwiać generowanie raportów z własnego działania zarówno w formie na żądanie jak i zaplanowanych z możliwością wysyłania wygenerowanego raportu na określony adres email,
20. rozwiązanie musi posiadać możliwość korelowania, priorytetyzacji i agregacji zdarzeń na bazie wszystkich dostępnych dla ATP źródeł,
21. rozwiązanie musi posiadać możliwość budowania mapy rozprzestrzeniania się zagrożenia,
22. rozwiązanie musi umożliwiać przeskanowanie objętej osłoną infrastruktury pod kątem wykrycia śladów działania zaawansowanych zagrożeń w zakresie sumy kontrolnej pliku, klucza rejestru,

określonej komunikacji sieciowej, określonych procesów czy innych, nie wskazanych tutaj indykatorów zagrożeń,

23. rozwiązanie musi w przypadku wykrycia zagrożenia na jednym z urządzeń współdzielić informacje o zagrożeniu z pozostałymi urządzeniami,
24. rozwiązanie musi umożliwiać analizę zarejestrowanych zachowań aplikacji na urządzeniu na bazie zapisów historycznych,
25. rozwiązanie musi być zasilane w aktualizacje zagrożeń przez Producenta,
26. rozwiązanie musi posiadać możliwość korelacji wykrytych zdarzeń ze znanymi indykatorami aktywności kampanii ATP,
27. rozwiązanie musi zachować pełną funkcjonalność w przypadku utraty komunikacji z systemami aktualizacji Producenta,
28. rozwiązanie musi posiadać system lokalnej oraz globalnej reputacji,
29. rozwiązanie musi posiadać możliwość tworzenia czarnych i białych list w oparciu o co najmniej sumy kontrolne plików,
30. rozwiązanie powinno umożliwiać sprawdzenie zagrożenia w bazie Virus Total lub inny o podobnej skali zastosowania wielu silników antywirusowych,
31. rozwiązanie musi posiadać możliwość zdetonowania potencjalnego zagrożenia w sandbox,
32. administrator musi posiadać opcję ręcznego wywołania analizy próbki zarówno dla pliku jak i URL w sandbox,
33. rozwiązanie po detonacji zagrożenia musi raportować źródłowe IP, docelowe IP, C&C, URL, klasę złośliwego oprogramowania, użyte protokoły,
34. sandbox musi posiadać możliwość dostosowania obrazów wirtualnych maszyn do środowiska produkcyjnego (stacji roboczej) Zamawiającego,
35. sandbox musi posiadać możliwość wykrycia zachowań zmierzających do detekcji środowiska uruchomienia próbki i tym samym stosować mechanizmy oszukujące oprogramowanie podlegające analizie,
36. rozwiązanie musi posiadać możliwość integracji z Active Directory,
37. rozwiązanie może być alokowane na zasobach fizycznych lub wirtualnych,
38. wszystkie dane w Rozwiązaniu, w szczególności informacje o objętych ochroną urządzeniach, zaistniałych zdarzeniach, dane raportowe oraz inne tu nie wyszczególnione muszą bezwzględnie być przechowywane i przetwarzane w środowisku on-premise,
39. rozwiązanie nie może wykorzystywać rozwiązań chmurowych jako komponentu systemu, niezbędnego do dostarczenia wskazanej funkcjonalności.

Wszystkie prace muszą odbywać się z uwzględnieniem zapewnienia ciągłości działania integrowanych z Rozwiązaniem systemów.

4. PRZEWIDYWANY HARMONOGRAM PRAC

Harmonogram prac dla implementacji rozwiązania systemu klasy Advanced Threat Protection (ATP)		
Lp.	**Nazwa**	**Czas trwania zadania**
Analiza (data końcowa etapu jest datą odbioru)		
1	Analiza rozwiązań funkcjonujących w Grupie Energa, z którymi zostanie wykonana integracja. Przygotowanie szczegółowego harmonogramu wdrożenia	2 tygodnie od momentu podpisania umowy
2	Przygotowanie dokumentacji przedwdrożeniowej zawierającej docelową architekturę wdrożenia	2 tygodnie od momentu zakończenia prac z pkt 1
Implementacja Rozwiązania ATP(data końcowa etapu jest datą odbioru)		
3	Dostarczenie platformy sprzętowej przez Zamawiającego, niezbędnej do realizacji wdrożenia, zgodnej z dokumentacją przedwdrożeniową. Szkolenie wstępne z produktu dla pracowników Zamawiającego	16 tygodni od momentu zakończenia prac z pkt 2
4	Instalacja elementów Rozwiązania zgodnie z przyjętą dokumentacją przedwdrożeniową	2 tygodnie od momentu zakończenia prac z pkt 3
5	Konfiguracja Rozwiązania zgodnie z przyjętą dokumentacją przedwdrożeniową	4 tygodnie od momentu zakończenia prac z pkt 4
6	Testy akceptacyjne	4 tygodnie od momentu zakończenia prac z pkt 5
7	Wdrożenie poprawek wynikających z testów akceptacyjnych	2 tygodnie od momentu zakończenia prac z pkt 6
Start produkcyjny i okres stabilizacji systemu (data końcowa etapu jest datą odbioru)		
8	Stabilizacja	3 tygodnie od momentu zakończenia prac z pkt 7
9	Szkolenie pracowników z wykorzystaniem funkcjonującego Rozwiązania	2 tygodnie od momentu zakończenia prac z punktu 8
10	Przygotowanie dokumentacji powdrożeniowej	2 tygodnie od momentu zakończenia prac z pkt 9

5. WYMAGANIA DOTYCZĄCE ODPOWIEDZI

1. Odpowiedź na zapytanie o informację należy przesłać drogą elektroniczną do dnia **18.06.2020** roku do godz. **14:00** na adres: Agnieszka.Gasior@energa.pl
2. Odpowiedź na zapytanie powinno zawierać, co najmniej:

a. Wypełniony Arkusz wyceny zgodnie z **Załącznikiem nr 2.**

3. Pytania dotyczące kwestii objętych niniejszym dokumentem można zadawać w terminie do dnia **15.06.2020** roku do godz. **12:00** kierując je do osoby uprawnionej do kontaktowania się z Wykonawcami zgodnie z pkt. 1 powyżej.
4. Zadawane pytania należy wpisać z wykorzystaniem szablonu określonego w **Załączniku nr 1** do Zapytania.
5. Pytania i udzielone przez EITE odpowiedzi zostaną przesłane do wszystkich Wykonawców w miarę możliwości niezwłocznie, bez ujawniania zadającego pytania, z zastrzeżeniem jak poniżej.

6. INFORMACJE DODATKOWE

1. Niniejszy dokument stanowi zapytanie informacyjnie (RFI), które nie stanowi zaproszenia do złożenia oferty w rozumieniu ustawy z dnia 23 kwietnia 1964 Kodeksu Cywilnego (tekst jednolity z 16 maja 2019 r., Dz. U. z 2019 r. poz. 1145 z późn. zm.).
2. Niniejsze Zapytanie o Informacje nie jest elementem jakiegokolwiek postępowania w rozumieniu ustawy z dnia 29 stycznia 2004r. Prawo zamówień publicznych (tekst jednolity z 11 września 2019 r., Dz. U. z 2019 r. poz. 1843 z późn. zm.).
3. Złożenie odpowiedzi na niniejsze Zapytanie o Informację jest jednoznaczne z wyrażeniem zgody przez podmiot składający odpowiedź na nieodpłatne wykorzystanie przez Zamawiającego wszystkich wskazanych w odpowiedzi na Zapytanie o Informację danych do ewentualnego przygotowania przez Zamawiającego opisu przedmiotu zamówienia, szacunkowej wartości zamówienia, warunków umowy lub innych dokumentów niezbędnych dla postępowania zakupowego z zastrzeżeniem, że Zamawiający nie ujawni podmiotom trzecim tych danych, a także źródła ich uzyskania.
4. Każdy podmiot, który otrzymał niniejsze Zapytanie, samodzielnie ponosi wszelkie koszty w związku z udziałem w Zapytaniu. Za udział w Zapytaniu podmioty w nim uczestniczące nie otrzymują wynagrodzenia.
5. Prosimy o przedstawienie najbardziej korzystnej dla ENERGA Informatyka i Technologie Sp. z o.o. odpowiedzi.

7. ZAŁĄCZNIKI

Integralną częścią niniejszego Zapytania o informację są wymienione poniżej Załączniki

Załącznik nr 1 - Arkusz pytań

Załącznik nr 2 - Arkusz wyceny