INSTYTUT PAMIĘCI NARODOWEJ
Komisja Ścigania Zbrodni
przeciwko Narodowi Polskiemu
Biuro Administracyjno Gospodarcze

Wszyscy uczestnicy postępowania
o udzielenie zamówienia publicznego

Pismo z dnia:	Znak:	Nasz znak:	Data:
		BAG-V4-280-35(24)/18	Warszawa, dnia 02.07.2018 r.

Dotyczy: postępowania o udzielenie zamówienia publicznego, prowadzonego w trybie przetargu nieograniczonego na: **„Zakup systemu zaawansowanej ochrony stacji użytkowników i serwerów dla IPN wraz z jego wdrożeniem"(BAG-31/18)**.

WYJAŚNIENIE ORAZ MODYFIKACJA TREŚCI SPECYFIKACJI ISTOTNYCH WARUNKÓW ZAMÓWIENIA

Instytut Pamięci Narodowej – Komisja Ścigania Zbrodni przeciwko Narodowi Polskiemu, ul. Wołoska 7, 02-675 Warszawa, działając na podstawie art. 38 ust. 1, 2 i 4 ustawy z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (Dz. U. z 2017 r., poz. 1579z póź. zm.) zawiadamia, że wpłynęły zapytania dotyczące treści Specyfikacji Istotnych Warunków Zamówienia, na które udzielono następujących odpowiedzi:

Pytanie 1:
Dotyczy pkt. XV SIWZ i pkt. 3 załącznika nr 2 do SIWZ, „Opis Przedmiotu Zamówienia".
Pozycja nr 2 tabeli „Funkcje dodatkowe" punktu XV. SIWZ, zawiera ogólny opis zagadnienia, które bardziej szczegółowo opisane jest w pkt 3 załącznika nr 2 do SIWZ „Opis Przedmiotu Zamówienia".
Czy Zamawiający rozumie zapisy zawarte w punkcie 3 załącznika nr 2 do SIWZ jako rozwinięcie opisu funkcji znajdującej się w 2 tabeli „Funkcje dodatkowe"?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że podtrzymuje zapisy SIWZ. Punkt XV opisuje dodatkowe kryteria funkcjonalności przedmiotowego systemu, które dodatkowo będą punktowane przez Zamawiającego.

Pytanie 2
Dotyczy pkt 2 podpunkt „e." Załącznika nr 2 do SIWZ, „Opis Przedmiotu Zamówienia".
Uprzejmie prosimy o informację, jaką wersję systemu operacyjnego Windows Server może udostępnić Zamawiający na potrzeby wdrożenia?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że dysponuje licencjami Windows Server Datacenter 2012 r2.

Pytanie 3
Dotyczy pkt 2 podpunkt „b." zał. Nr 2 do SIWZ, „Opis Przedmiotu Zamówienia".
Zamawiający określa w zapisie w ww. punkcie, że: „rozwiązanie powinno posiadać 3-warstwową architekturę składającą się z konsoli, serwera zarządzania oraz serwera bazy danych. Rozwiązanie powinno umożliwiać instalację i uruchomienia wszystkich trzech komponentów na jednym serwerze sprzętowym

INSTYTUT PAMIĘCI NARODOWEJ – KOMISJA ŚCIGANIA ZBRODNI PRZECIWKO NARODOWI POLSKIEMU
Biuro Administracyjno Gospodarcze
ul. Wołoska 7, 02-675 Warszawa, tel. (022) 581-8803, fax. (022) 581-88-14
www.ipn.gov.pl

/ wirtualnym lub instalację rozproszoną". Uprzejmie prosimy o informację jakie licencje SQL dostępne na platformę Windows Server posiada Zamawiający?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że jest w stanie zapewnić Microsoft SQL Express na platformę Windows Server.

Pytanie 4

Uprzejmie prosimy Zamawiającego o udostępnienie formularza ofertowego w pliku edytowalnym o rozszerzeniu „.doc".

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że udostępnia dokumentację postępowania o udzielenie zamówienia publicznego jedynie w formie plików otwartych.

Pytanie 5

Po przeanalizowaniu zapytania stwierdzamy, że jedynym rozwiązaniem spełniającym wymagania jest rozwiązanie PaloAlto Traps.
Rozwiązania do ochrony stacji końcowych PaloAlto według niezależnych konsultantów (np. Gartner) uznawane są raczej za rozwiązania niszowe a nie zaawansowane tak jak wskazuje nazwa Państwa zapytania.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, iż nie może ustosunkować się do ww. sugestii ze względu na brak pytania.

Pytanie 6

Punkt 3 h) Załącznika nr 2 do SIWZ ogranicza konkurencyjność, ponieważ wyłącznym produktem spełniającym ten zapis jest Palo Alto Traps. Również punkt 7 c) Załącznika nr 2 do SIWZ jednoznacznie wskazuje na Palo Alto Traps. Pomimo że Microsoft Defender Advanced Threat Protection także spełnia ten punkt, lecz z kolei nie spełnia wielu pozostałych wymienionych w Załączniku nr 2 do SWIZ. Między innymi takich jak punkt 2 b), c), e), f), ponieważ jest to usługa hostowana w chmurze Microsoft, a jedynie agenci chroniący są instalowani na systemach chronionych.

Zgodnie z art. 29 ust. 2 PZP przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję. Oznacza to w szczególności zakaz posługiwania się przez zamawiających przy określaniu przedmiotu zamówienia jakimikolwiek sformułowaniami lub parametrami, które wskazywałby na konkretny wyrób, produkt, czy też wykonawcę. W związku z powyższym prosimy o wykreślenie podpunktu c w punkcie 7 oraz zmianę treści podpunktu h w punkcie 3c na przykładową: „Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela i powinno działać na komputerach posiadających minimalnie 512MB RAM i procesor Intel Pentium 4.".

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że dokonuje stosownych zmian w załączniku nr 2 do SIWZ - Opis przedmiotu zamówienia i nie wskazuje na konkretne rozwiązania.

Było:

3. h. Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

7. c. Zaproponowane rozwiązanie musi umożliwiać użycie usługi inteligentnego transferu w tle – BITS (Background Intelligence Transfer Service) przy wykorzystaniu przeglądarki web oraz umożliwiać przesyłanie danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego.

Jest:

3. h. Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 2% a zajętość pamięci RAM nie więcej niż 100MB.

7. c. Zaproponowane rozwiązanie musi umożliwiać użycie usługi inteligentnego transferu w tle przy wykorzystaniu przeglądarki web oraz umożliwiać przesyłanie danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego.

Pytanie 7
Wymagania wskazują na rozwiązanie PaloAlto Traps. Czy dopuszczają Państwo inne rozwiązania do ochrony punktów końcowych?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że nie wskazuje na konkretne rozwiązania.

Pytanie 8
OPZ pkt. 1

W OPZ piszą Państwo:

b. Proponowane rozwiązanie powinno posiadać 3-warstwową architekturę składającą się z konsoli, serwera zarządzania oraz serwera bazy danych. Rozwiązanie powinno umożliwiać instalację i uruchomienia wszystkich trzech komponentów na jednym serwerze sprzętowym / wirtualnym lub instalację rozproszoną.

Prosimy o zmianę powyższych zapisów na:

b. Proponowane rozwiązanie powinno posiadać 3-warstwową architekturę składającą się z konsoli, serwera zarządzania oraz serwera bazy danych. Rozwiązanie powinno umożliwiać instalację i uruchomienia wszystkich trzech komponentów na jednym serwerze sprzętowym / wirtualnym lub instalację rozproszoną. Zamawiający dopuszcza rozwiązanie, którego zarządzanie stacjami końcowymi odbywać się będzie w środowisku chmurowym bez konieczności instalacji dedykowanego serwera zarządzającego, bazy danych i konsoli w środowisku Zamawiającego.

Odpowiedź:

W odpowiedzi na powyższą prośbę, Zamawiający wyjaśnia, że podtrzymuje zapisy SIWZ.

Pytanie 9
OPZ pkt. 2
c. Proponowane rozwiązanie powinno umożliwiać instalację wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli.

Prosimy o zmianę powyższych zapisów na:

c. Proponowane rozwiązanie powinno umożliwiać instalację wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli. Zamawiający dopuszcza rozwiązanie instalacji jednego serwera zarządzającego wraz z dodatkowymi serwerami pośredniczącymi, które będą optymalizowały pracę odległych oddziałów oraz będą podlegały głównemu serwerowi.

Odpowiedź:

W odpowiedzi na powyższą prośbę, Zamawiający wyjaśnia, że wyraża zgodę na zaproponowane zmiany w pkt 2 załącznika nr 2 do SIWZ – Opis przedmiotu zamówienia i dokonuje stosownych zmian.

Było:

c. Proponowane rozwiązanie musi umożliwiać instalację wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli.

Jest:

c. Proponowane rozwiązanie powinno umożliwiać instalację wielu serwerów zarządzania w konfiguracji rozproszonej i zarządzanie nimi z poziomu pojedynczej konsoli. Zamawiający dopuszcza rozwiązanie instalacji jednego serwera zarządzającego wraz z dodatkowymi serwerami pośredniczącymi, które będą optymalizowały pracę odległych oddziałów oraz będą podlegały głównemu serwerowi.

Pytanie 10
OPZ pkt. 2

e. Proponowane rozwiązanie powinno być rozwiązaniem programowym działającym na systemie operacyjnym Windows Server.

Prosimy o zmianę powyższych zapisów na:

e. Proponowane rozwiązanie powinno być rozwiązaniem programowym działającym na systemie operacyjnym Windows Server. Zamawiający dopuszcza rozwiązanie programowe działające na systemie operacyjnym Linux w formie gotowej wirtualnej maszyny VMWare.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że podtrzymuje zapisy SIWZ.

Pytanie 11

f. Proponowane rozwiązanie powinno dawać możliwość uruchomienia w środowisku zwirtualizowanym (np. VMWare).
Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

Pytanie:

Czy Zamawiający dopuści rozwiązanie, którego zajętość procesora będzie wynosić 1% a zajętość pamięci RAM nie więcej niż 20MB, ale rozwiązanie będzie bez lokalnego interfejsu graficznego?

Ewentualnie prosimy o zmianę aby ten pkt brzmiał:

f. Proponowane rozwiązanie powinno dawać możliwość uruchomienia w środowisku zwirtualizowanym (np. VMWare).
Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 2% a zajętość pamięci RAM nie więcej niż 100MB.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Pytanie 12

a. Proponowane rozwiązanie powinno posiadać opcję integracji ze stosowanym w organizacji chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

Pkt. ten sugeruje, że Zamawiający oczekuje dostarczenia produktu tego samego producenta co środowiska wykrywania ataków APT z którego obecnie korzysta.

Specjalizując się w tematyce bezpieczeństwa IT od 15 lat, informujemy, że każdy producent używa swojego, własnego środowiska APT tj. PaloAlto – Wildfire, Checkpoint – Sandblast, itd., więc niemożliwym jest dostarczenie rozwiązań innego producenta co kłóci się z zasadą zachowania konkurencyjności, dlatego prosimy o zmianę tego zapisu na:

a. Proponowane rozwiązanie powinno posiadać możliwość łączenia się z chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że nie wskazuje na konkretne rozwiązania i dokonuje stosownych modyfikacji w załączniku nr 2 do SIWZ – Opis przedmiotu zamówienia.

Było:

a. Proponowane rozwiązanie musi posiadać opcję integracji ze stosowanym w organizacji chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

Jest:

a. Proponowane rozwiązanie powinno posiadać możliwość integracji z chmurą producenta oferowanego rozwiązania, w której wykrywane byłyby ataki aplikacyjne. Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do ww. środowiska chmurowego.

Pytanie 13

Wyłącznie produkt Palo Alto Traps spełnia wymagania opisane w Załącznika nr 2, pkt. 3, ppkt. h do SIWZ co ogranicza konkurencyjność postępowania i jednoznacznie wskazuje na wyżej wymieniony produkt. Także pkt. 7, ppkt. c przedmiotowego załącznika jednoznacznie wskazuje na Palo Alto Traps, co również wyklucza złożenie oferty na innym rozwiązaniu niż Palo Alto Traps, co kolejny raz skutkuje eliminacją pozostałych rozwiązań konkurencyjnych. W celu dochowania rzetelności należy stwierdzić iż, pomimo że Microsoft Defender Advanced Threat Protection spełnia ten punkt, to nie spełnia innych punktów/wymagań wymienionych w Załączniku nr 2, np.: punkt 2 b, ci wiele innych.

Mając na uwadze art. 29 ust. 2 PZP przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudnić uczciwą konkurencję. Powyższy artykuł oznacza również zakaz posługiwania się przez zamawiającego przy opisywaniu przedmiotu zamówienia sformułowaniami czy też parametrami, które wskazują na konkretny wyrób, produkt, czy też wykonawcę. W związku z tym proszę o usunięcie zapisu w pkt. 7, ppkt. ci pkt. 3, ppkt. h, lub zmianę treści pkt. 3, ppkt. h na zapis umożliwiający złożenie oferty na rozwiązaniu innym niż Palo Alto Traps. Powyższe umożliwi uczciwą konkurencję i doprowadzi do zgodności zapisów postępowania z wymogami PZP .

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Pytanie 14

Wyłącznie produkt Palo Alto Traps spełnia wymagania opisane w Załącznika nr 2, pkt. 3, ppkt. h do SIWZ co ogranicza konkurencyjność postępowania i jednoznacznie wskazuje na wyżej wymieniony produkt. Także pkt. 7, ppkt. c przedmiotowego załącznika jednoznacznie wskazuje na Palo Alto Traps, co również wyklucza złożenie oferty na innym rozwiązaniu niż Palo Alto Traps, co kolejny raz skutkuje eliminacją pozostałych rozwiązań konkurencyjnych. W celu dochowania rzetelności należy stwierdzić iż, pomimo że Microsoft Defender Advanced Threat Protection spełnia ten punkt, to nie spełnia innych punktów/wymagań wymienionych w Załączniku nr 2, np.: punkt 2 b, ci wiele innych.

Mając na uwadze art. 29 ust. 2 PZP przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudnić uczciwą konkurencję. Powyższy artykuł oznacza również zakaz posługiwania się przez zamawiającego przy opisywaniu przedmiotu zamówienia sformułowaniami czy też parametrami, które wskazują na konkretny wyrób, produkt, czy też wykonawcę. W związku z tym proszę o usunięcie zapisu w pkt. 7, ppkt. ci pkt. 3, ppkt. h, lub zmianę treści pkt. 3, ppkt. h na zapis umożliwiający złożenie oferty na rozwiązaniu innym niż Palo Alto Traps. Powyższe umożliwi uczciwą konkurencję i doprowadzi do zgodności zapisów postępowania z wymogami PZP .

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Pytanie 15

Dotyczy wymagania : 3. h. Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

Czy wymaganie dotyczy pracy w trybie bezczynności?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Pytanie 16

Dotyczy wymagania 5. a. Proponowane rozwiązanie powinno posiadać opcję integracji ze stosowanym w organizacji chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

Jakie rozwiązanie jest stosowane w organizacji do wykrywania ataków APT?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 17

Dotyczy wymagania 5. b. Proponowane rozwiązanie powinno posiadać możliwość weryfikacji w chmurowym środowisku anty-APT czy dany plik jest złośliwy, czy legalny na bazie skrótu cyfrowego pliku.

Czy wymaganie dotyczy stosowanego w organizacji rozwiązania anty APT (zgodnie z punktem 5a). Czy dotyczy innego oferowanego przez oferenta rozwiązania?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 18

Dotyczy wymagania 5. c. Proponowane rozwiązanie powinno posiadać możliwość wysłania poprzez serwer zarządzania potencjalnie złośliwego pliku do analizy w chmurowym środowisku antyAPT.

Czy wymaganie dotyczy stosowanego w organizacji rozwiązania anty APT (zgodnie z punktem 5a). Czy dotyczy innego oferowanego przez oferenta rozwiązania?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 19

Dotyczy wymagania 5. d. Proponowane rozwiązanie powinno posiadać możliwość wglądu w raport wynikowy analizy pliku w środowisku chmurowym anty-APT bezpośrednio z poziomu stacji zarządzania oprogramowaniem zabezpieczeń stacji końcowych.

Czy wymaganie dotyczy stosowanego w organizacji rozwiązania anty APT (zgodnie z punktem 5a). Czy dotyczy innego oferowanego przez oferenta rozwiązania?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 20

Dotyczy wymagania 5. e. Proponowane rozwiązanie nie powinno analizować w środowisku chmurowym plików, które były w nim analizowane uprzednio. Powinien działać mechanizm powiadamiania, iż dany plik był już wcześniej poddawany analizie.

Czy wymaganie dotyczy stosowanego w organizacji rozwiązania anty APT (zgodnie z punktem 5a). Czy dotyczy innego oferowanego przez oferenta rozwiązania?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 21

Dotyczy wymagania 6. c. Zaproponowane rozwiązanie powinno umożliwiać użycie usługi inteligentnego transferu w tle – BITS (Background Intelligence Transfer Service) przy wykorzystaniu przeglądarki web oraz umożliwiać przesyłanie danych powiązanych z dokumentacją dowodową za pomocą niewykorzystanego pasma sieciowego.

Czy dopuszczalne jest wykorzystanie innego protokołu wymiany informacji niż BITS?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że Wykonawcy chodzi zapewne o pkt 7 c załącznika nr 2 do SIWZ – Opis przedmiotu zamówienia oraz, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 12.

Pytanie 22

Dotyczy wymagania 6. f. Zaproponowane rozwiązanie powinno umożliwiać automatyczne tworzenie wyjątków odnośnie reguł oraz skrótów cyfrowych bezpośrednio z raportu dotyczącego wykrytego zagrożenia w celu umożliwienia uruchomienia danego procesu na poszczególnych stacjach końcowych.

Czy wymaganie dotyczy tylko modułu Forensics czy innych wymaganych modułów ochrony?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, iż Wykonawcy chodzi zapewne o pkt 7 f załącznika nr 2 do SIWZ – Opis przedmiotu zamówienia jednocześnie wyjaśnia, iż dotyczy to modułu Forensic.

Pytanie 23

Dot.: Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

Czy Zamawiający oczekuje, że proponowane rozwiązanie będzie utrzymywać taki poziom zajętości zasobów niezależnie od tego jakie zadania i analizy wykonuje system w danym momencie, czy jest to poziom oczekiwany dla stanu, kiedy na stacji użytkownika, nie są wykonywane żadne akcje? Jakie parametry sprzętowe procesora Zamawiający uznaje jako referencyjne oraz dla jakiego systemu operacyjnego (nazwa, wersja) Zamawiający przyjmuje dla ww. wymagania?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Zamawiający ponadto informuje, iż powyższe wartości są traktowane jako referencyjne dla systemu operacyjnego Windows 7, 8, 10.

Pytanie 24

Dot.: Proponowane rozwiązanie nie może znacząco obciążać zasobów sprzętowych komputera nosiciela, tj. zajętość procesora nie może wynosić więcej niż 1% a zajętość pamięci RAM nie więcej niż 20MB.

Czy ograniczenie na 20MB dotyczy pamięci fizycznej RAM, czy łącznie pamięci RAM i pamięci wirtualnej?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6 i 23.

Pytanie 25

Dot.: Proponowane rozwiązanie powinno aktualizować moduły blokowania technik ataków nie częściej niż raz na 6 miesięcy, tak aby minimalizować narzut czynności administracyjnych i operacyjnych związanych z aktualizacjami.

Czy wymaganie na minimalny okres 6 miesięcy między kolejnymi aktualizacjami modułów blokowania technik ataków Zamawiający uważa za wystarczający? Jaka będzie skuteczność systemu jeśli nowe techniki pojawią się między kolejnymi aktualizacjami?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, iż dokonuje stosownych modyfikacji w załączniku nr 2 do SIWZ – Opis przedmiotu zamówienia.

Było

3. j. Proponowane rozwiązanie powinno aktualizować moduły blokowania technik ataków nie częściej niż raz na 6 miesięcy, tak aby minimalizować narzut czynności administracyjnych i operacyjnych związanych z aktualizacjami.

Jest:

3. j. Proponowane rozwiązanie powinno aktualizować moduły blokowania technik ataków zgodnie z rekomendacją producenta oferowanego systemu, tak aby minimalizować narzut czynności administracyjnych i operacyjnych związanych z aktualizacjami.

Pytanie 26

Jaką ilość użytkowników stacji końcowych posiada zamawiający?

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, iż informacja o ilości stacji końcowych jest podana w SIWZ: pkt. III 1. oraz Załączniku nr 2 (OPZ) pkt 1.

Pytanie 26

5. Wykrywania nieznanych złośliwych kodów wykonywalnych.
a) Proponowane rozwiązanie powinno posiadać opcję integracji ze stosowanym w organizacji chmurowym środowiskiem wykrywania ataków typu APT (Advanced Persistent Threat). Jednocześnie proponowane rozwiązanie musi zapewniać skuteczną ochronę przeciwko złośliwemu oprogramowaniu oraz atakom aplikacyjnym nawet jeśli nie posiada połączenia do środowiska chmurowego.

Pytanie
Z wymagania wynika, że Zamawiający posiada chmurowe środowisko wykrywania ataków typu APT. Prosimy o przytoczenie nazwy tego środowiska, wersji oraz producenta w celu umożliwienia oceny możliwości spełnienia tego wymagania przez proponowane rozwiązanie.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 16.

Pytanie 27

5. Wykrywania nieznanych złośliwych kodów wykonywalnych.
b. Proponowane rozwiązanie powinno posiadać możliwość weryfikacji w chmurowym środowisku anty-APT czy dany plik jest złośliwy, czy legalny na bazie skrótu cyfrowego pliku.
c. Proponowane rozwiązanie powinno posiadać możliwość wysłania poprzez serwer zarządzania potencjalnie złośliwego pliku do analizy w chmurowym środowisku anty-APT.
d. Proponowane rozwiązanie powinno posiadać możliwość wglądu w raport wynikowy analizy pliku w środowisku chmurowym anty-APT bezpośrednio z poziomu stacji zarządzania oprogramowaniem zabezpieczeń stacji końcowych.
e. Proponowane rozwiązanie nie powinno analizować w środowisku chmurowym plików, które były w nim analizowane uprzednio. Powinien działać mechanizm powiadamiania, iż dany plik był już wcześniej poddawany analizie.
f. Proponowane rozwiązanie powinno posiadać możliwość zapobiegania nieznanym złośliwym plikom wykonywalnym poprzez zastosowanie chmurowego środowiska anty-APT typu „sandbox". Dodatkowo powinna istnieć możliwość przedstawienia wyniku analizy pliku wraz z pełnym raportem z analizy.
g. Proponowane rozwiązanie powinno posiadać możliwość ręcznego dostrojenia lub nadpisania werdyktu będącego wynikiem analizy w środowisku chmurowym dla konkretnego skrótu cyfrowego pliku.
h. Proponowane rozwiązanie powinno posiadać możliwość zablokowania uruchomienia pliku wykonywalnego jeśli skrót cyfrowy pliku jest nieznany, tj. plik ten nie był uprzednio analizowany w środowisku chmurowym anty-APT producenta.
Pytanie 1
Z wymagania wynika, że Zamawiający posiada chmurowe środowisko wykrywania ataków typu APT. Prosimy o przytoczenie nazwy tego środowiska, wersji oraz producenta w celu umożliwienia oceny możliwości spełnienia tego wymagania przez proponowane rozwiązanie.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 16.

Pytanie 28

Czy wspomniane w powyższych wymaganiach środowisko chmurowe anty--□APT powinny być funkcjonalnością dostarczanego rozwiązania? Czy Za mawiający posiada własne rozwiązanie tego typu? Jeśli tak to prosimy o podanie nazwy, wersji oraz producenta.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 16.

Pytanie 29

Czy proponowane rozwiązanie powinno posiadać funkcjonalność chroniącą przed nietypowymi zachowaniami użytkowników (np. wizyty na „niebezpiecznych stronach")?

Odpowiedź:

W odpowiedzi na powyższe pytania, Zamawiający wyjaśnia, iż podtrzymuje zapisy SIWZ.

Pytanie 30

Zgodnie z zapisami art. 29 ust. 2 PZP przedmiot zamówienia nie może być opisywany w sposób, który utrudnia uczciwą konkurencję. Skutkuje to również zakazem posługiwania się przez zamawiającego, przy opisywaniu przedmiotu zamówienia, sformułowaniami czy też parametrami, które wskazują na konkretny wyrób, produkt, czy też wykonawcę.
Wymagania opisane w Załączniku nr 2 do SIWZ: pkt. 3.h i 7 .c jednoznacznie wskazują, że jedynym rozwiązaniem spełniającym wymagania SIWZ jest produkt Palo Alto Traps. Są wiec one sformułowane sprzecznie z zapisami art. 29 ust. 2 PZP, gdyż wykluczają uczciwą konkurencję i wskazują na konkretny produkt.
W związku z tym proszę o usunięcie punktów: pkt. 3.h 7.c co będzie skutkować umożliwieniem uczciwej konkurencji zgodnie z zapisami PZP.

Odpowiedź:

W odpowiedzi na powyższe pytanie, Zamawiający wyjaśnia, że odpowiedź jest tożsama z odpowiedzią na pytanie nr 6.

Zastępca Dyrektora Biura
Administracyjno-Gospodarczego
Robert Kuźma