Warszawa, dnia 20.11.2020 r.

Wyjaśnienia SIWZ

Działając na podstawie art. 38 ust. 1, i 2 ustawy Prawo zamówień publicznych (Dz. U. z 2019 r. poz. 1843, z późn. zm.), Zamawiający odpowiada na pytania do SIWZ zadane przez wykonawców w postępowaniu o udzielenie zamówienia pn.: ***„Dostawa i wdrożenie „Systemu Bezpiecznego Dostępu do Sieci Internet”,*** *numer sprawy:* ***70/ST/KSZBI/POPC/PN/2020***, ogłoszenie o zamówieniu numer 2020/S 220-539778 z dnia 11-11-2020 r.

Pytanie 1:
Dotyczy A1.8
Dedykowane proxy dla protokołów strumieniowych – MMS, RTSP, RTMP, HLS, HDS i Silverlight.
Czy zamawiający dopuści rozwiązanie nie posiadające dedykowanych systemów proxy dla protokołów strumieniowych jednak umożliwiające obejście (tunelowanie) proxy dla tych protokołów?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie nie posiadające dedykowanych systemów proxy dla protokołów strumieniowych jednak umożliwiające obejście (tunelowanie) proxy dla tych protokołów.

Pytanie 2:
Dotyczy A1.18
Niezależnie od mechanizmu klasyfikacji w oparciu o kategorię strony musi istnieć mechanizm oceny reputacji danej strony uwzględniający przynajmniej 5 stopni ryzyka.
Czy zamawiający dopuści rozwiązanie nie posiadające dodatkowego mechanizmu oceny ryzyka jednak posiadające 3 stopniową ocenę ryzyka aplikacji cloud?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie nie posiadające dodatkowego mechanizmu oceny ryzyka jednak posiadające 3 stopniową ocenę ryzyka aplikacji cloud.

Pytanie 3:
Dotyczy A1.19
Możliwość konstrukcji polityki w oparciu o reputację danej strony w połączeniu z bazą kategorii np. blokuj reklamy ze stron o średnim lub wysokim poziomie ryzyka.
Czy zamawiający dopuści rozwiązanie posiadające dodatkowo blokowanie za pomocą filtrów tekstowych oraz regex zamiast blokady poziomów ryzyka?
Odpowiedź Zamawiającego:
Zamawiający dopuści filtry tekstowe oraz regex, jako dodatkowe do filtrów reputacyjnych wymaganych w OPZ.

Pytanie 4:
Dotyczy A1.23
Rozwiązanie musi mieć możliwość tworzenia polityk w oparciu o geolokalizację.
Czy zamawiający dopuści możliwość definiowania lokalizacji przetwarzających ruch http/s za pomocą różnych systemów proxy w organizacji, a w przypadku implementacji cloud lub hybrydowej wybór najbliżej oddalonego geograficznie centrum przetwarzania proxy w chmurze?
Odpowiedź Zamawiającego:

Zamawiający przez geolokalizację rozumie wykrywanie geograficznej lokalizacji docelowych stron internetowych, do których odbywa się ruch z organizacji zamawiającego. W oparciu o tą geolokalizacje w systemie musi istnieć możliwość tworzenia polityk.

Pytanie 5:
Dotyczy A1.35
Zarządzanie pasmem musi działać dla protokołów strumieniowych tj. MMS, RTSP, RTMP, HLS i HDS.
Czy zamawiający dopuści rozwiązanie nie posiadające zarządzania pasma dla protokołów strumieniowych jednak umożliwiające obejście (tunelowanie) proxy dla tych protokołów?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie nie posiadające zarządzenia pasmem dla protokołów strumieniowych, umożliwiające tunelowanie ruchu dla protokołów strumieniowych.

Pytanie 6:
Dotyczy A1.36
Rozwiązanie musi współpracować z zewnętrznymi skanerami antywirusowymi/antymalware za pomocą otwartego protokołu ICAP w tym jego szyfrowanej implementacji ICAPS.
Czy zamawiający dopuści rozwiązanie posiadające jedynie implementacje nieszyfrowaną protokołu ICAP?
Odpowiedź Zamawiającego:
Zamawiający dopuści jedynie nieszyfrowaną wersją protokołu ICAP.

Pytanie 7:
Dotyczy A1.37
System musi wspierać zarówno ICAP(S) request mode jak i ICAP(S) response mode.
Czy zamawiający dopuści rozwiązanie posiadające jedynie implementacje nieszyfrowaną protokołu ICAP?
Odpowiedź Zamawiającego:
Zamawiający dopuści jedynie nieszyfrowaną wersją protokołu ICAP.

Pytanie 8:
Dotyczy A1.40
Wsparcie wielu plików PAC w zależności od podsieci, w której znajduje się użytkownik.
Czy zamawiający ma na myśli rozwiązanie posiadające osobne (niezależne) komponenty proxy w różnych podsieciach posiadające osobne pliki PAC o niezależnej konfiguracji?
Odpowiedź Zamawiającego:
System powinien umożliwiać definicję plików PAC dla każdej z podsieci indywidualnie.

Pytanie 9:
Dotyczy A2.1.b
2 silniki AV działające jednocześnie, pochodzące od różnych producentów
Czy zamawiający dopuści rozwiązanie posiadające własny system AV oraz antymalware nie posiłkujący się rozwiązaniami 3-rd party?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Zamawiający wymaga działania 2 silników AV jednocześnie od dwóch różnych producentów. Rozwiązanie może posiadać własny system AV i dodatkowo innego producenta. Dwa niezależne mechanizmy skanowania antywirusowego zapewniają zwiększoną ochronę przed zagrożeniami, w przypadku gdy jeden z producentów nie uwzględnił w swoim rozwiązaniu tego typu zagrożenia.

Pytanie 10:
Dotyczy A2.1.c
inline sandboxing bez infekcji pacjenta zerowego – nie dopuszcza się rozwiązania chmurowego.

Czy Zamawiający w ramach systemu Antymalware miał namyśli dodatkowy sandboxing plików osobny od opisywanego poniżej systemu sandbox?

Odpowiedź Zamawiającego:

Zamawiający nie miał na myśli dodatkowego sandboxingu. Tą funkcję powinien realizować sandbox wymieniony w OPZ.

Pytanie 11:

Dotyczy A2.1.d

własna baza hash'y działająca na zasadzie białej / czarnej listy. Przy czym wspierane muszą być hash'e tworzone za pomocą algorytmu MD5 i SHA256

Czy zamawiający dopuści rozwiązanie posiadające tylko jeden z wymienionych algorytmów hash?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy OPZ. Wymienione powyżej algorytmy są wykorzystywane przez Zamawiającego. Do blokowania plików wykorzystywane są obie metody szyfrowania.

Pytanie 12:

Dotyczy A2.9

System musi być w stanie obsłużyć minimum 100 Mbps ruchu przy wykorzystaniu dwóch silników AV.

Czy zamawiający dopuści rozwiązanie posiadające własny system AV oraz antymalware nie posiłkujący się rozwiązaniami 3-rd party?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy OPZ. Zamawiający wymaga działania 2 silników AV jednocześnie od dwóch różnych producentów. Rozwiązanie może posiadać własny system AV i dodatkowo innego producenta. Dwa niezależne mechanizmy skanowania antywirusowego zapewniają zwiększoną ochronę przed zagrożeniami, w przypadku gdy jeden z producentów nie uwzględnił w swoim rozwiązaniu tego typu zagrożenia.

Pytanie 13:

Dotyczy B1.3

Wbudowana baza danych o wielkości co najmniej 1 TB.

Czy zamawiający dopuści rozwiązanie zainstalowane na platformie Windows Serwer w ramach posiadanych przez zamawiającego zasobów wykorzystujące serwer bazy Microsoft SQL Express lub posiadany przez zamawiającego serwer Microsoft SQL?

Odpowiedź Zamawiającego:

Zamawiający dopuszcza użycie bazy danych zamawiającego MS SQL Server 2019.

Pytanie 14:

Dotyczy B1.14.n

Czego szukają użytkownicy w Google, Bing itd.

Czy zamawiający dopuści rozwiązanie nie posiadające statystyk dla wyszukiwanych w przeglądarkach słów? Element ten nie jest związany z podnoszeniem bezpieczeństwa ani badania produktywności użytkowników.

Odpowiedź Zamawiającego:

Zamawiający dopuści rozwiązanie nie posiadające statystyk dla wyszukiwanych w przeglądarkach słów.

Pytanie 15:

Dotyczy B2.12

Szyfrowanie backupu urządzeń i systemu zarządzania.

Czy zamawiający dopuści rozwiązanie podsiadające możliwość backupu bez jego szyfrowania?

Odpowiedź Zamawiającego:

Zamawiający dopuści rozwiązanie nie posiadające możliwości szyfrowania backupu. W tym wypadku Zamawiający wymaga szyfrowanej komunikacji w trakcie przesyłania backupu**.**

Pytanie 16:
Dotyczy B2.15
Synchronizacja czasu z serwerem NTP
Czy zamawiający dopuści rozwiązanie wspierające NTP w ramach serwera, na którym uruchomiony jest system zarządzania?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie wspierające NTP w ramach serwera, na którym uruchomiony jest system zarządzania, pod warunkiem synchronizacji czasu tego serwera z serwerem Zamawiającego.

Pytanie 17:
Dotyczy B2.16
Monitorowanie przy pomocy SNMP poprzez odpytywanie bazy MIB
Czy zamawiający dopuści monitorowanie za pomocą wewnętrznych protokołów oferowanego rozwiązania?
Odpowiedź Zamawiającego:
Zamawiający dopuści monitorowanie za pomocą wewnętrznych protokołów oferowanego rozwiązania.

Pytanie 18:
Dotyczy C.1
Minimum dwóch fizycznych urządzeń tego samego typu pracujących w klastrze o wysokiej dostępności (HA) w trybie active-standby z możliwością realizacji trybu active-active – konieczna jest praca w konfiguracji odpornej
na awarie (wykrywanie uszkodzeń elementów sprzętowych i programowych oraz łączy sieciowych). Zamawiający nie przewiduje pracy urządzeń w trybie poza klastrem.
Czy zamawiający dopuści rozwiązanie posiadające możliwość tylko pracy w clustrze typu Active standby?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie posiadające możliwość tylko pracy w clustrze typu Active standby

Pytanie 19:
Dotyczy C.7
Dwa niezależne mechanizmy dynamicznej analizy plików tj. emulacja i wirtualizacja.
Czy zamawiający dopuści rozwiązanie posiadające tylko jeden z wymienionych mechanizmów analizy plików?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Do analizy może być wykorzystywana jedna z metod skonfigurowana przez zamawiającego. Planowane jest wykorzystanie emulacji lub wirtualizacji naprzemiennie, w zależności od krytyczności zabezpieczanego systemu i niezbędnej wydajności do analizy.

Pytanie 20:
Dotyczy C.9
Wymagane jest pełne dostosowywanie profili maszyn wirtualnych Windows 7/8/10 poprzez możliwość instalacji własnych aplikacji, określonych wersji Java, Flash Player itp. odpowiadających środowisku produkcyjnemu.
Czy zamawiający dopuści rozwiązanie posiadające emulacje dowolnych środowisk sprzętowo- programowych jednak nie posiadające możliwości instalacji własnej aplikacji?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Zamawiający jest autorem własnych aplikacji, dla których musi istnieć możliwość konfigurowania systemów bezpieczeństwa.

Pytanie 21:
Dotyczy C.10
System nie może ograniczać ilości profili wirtualnych maszyn poza dostępną przestrzenią dyskową tj. np. musi dać się stworzyć wiele różnych profili Windows 7/8/10 w celu odzwierciedlenia zróżnicowania konfiguracji stacji końcowych w organizacji.
Czy zamawiający dopuści rozwiązanie posiadające emulacje dowolnych środowisk sprzętowo- programowych jednak nie posiadające możliwości instalacji własnej konfiguracji systemu?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Zamawiający posiada różne konfiguracje systemów operacyjnych Windows 7/8/10, dla których musi istnieć możliwość konfigurowania systemów bezpieczeństwa.

Pytanie 22:
Dotyczy C.11
Możliwość dodawania własnych opisów zachowań złośliwego kodu i przypisania im określonego ryzyka.
Czy zamawiający dopuści rozwiązanie posiadające emulacje dowolnych środowisk sprzętowo- programowych jednak nie posiadające możliwości dodawania zachowań złośliwego kodu ani przypisywania ryzyk?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Ze względów bezpieczeństwa przypisanie poziomu ryzyka do określonego zachowania złośliwego kody jest konieczne.

Pytanie 23:
Dotyczy C.14
Musi istnieć możliwość konfiguracji Firewalla na ruchu wychodzącym z wirtualnych maszyn, w tym całkowitego odcięcia malware od komunikacji ze światem zewnętrznym, nawet przez dedykowany interfejs.
Czy zamawiający dopuści rozwiązanie posiadające już mechanizm odcięcia malware od świata zewnętrznego jednak nie posiadające mechanizmu konfiguracji firewalla?
Odpowiedź Zamawiającego:
Zamawiający dopuści za równoważne rozwiązanie mechanizmu odcięcia malware od świata zewnętrznego zaimplementowane w rozwiązaniu.

Pytanie 24:
Dotyczy C.15
System musi umożliwiać określenie czasu dynamicznej analizy / detonacji plików.
Czy zamawiający ma na myśli określenie maksymalnego czasu detonacji?
Odpowiedź Zamawiającego:
Zamawiający wyjaśnia, że wymaganie dotyczy możliwości wyboru momentu czasu analizy / detonacji plików.

Pytanie 25:
Dotyczy C.16
Pliki ściągane przez malware pierwszej fazy (dropper/loader) muszą być zapisywane w celu dalszej analizy.
Czy zamawiający dopuści rozwiązanie, gdzie pliki droperfile nie są ściągane?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Ze względów bezpieczeństwa musi istnieć możliwość dalszej analizy zagrożenia dotyczącego pobranych plików.

Pytanie 26:
Dotyczy C.19
Musi istnieć możliwość rozbudowy funkcjonalności systemu poprzez dodawanie pluginów, które wykonają się podczas procesu detonacji w celu wykonania jakiejś konkretnej czynności – np. dodatkowej interakcji z malware albo wyciągnięcia określonych danych z pamięci ulotnej.

Czy Zamawiający dopuści rozwiązanie posiadające mechanizmy dynamicznej emulacji dowolnych wzorców zachowań i dynamicznego podstawiania dowolnego sprzętu i oprogramowania bez możliwości dodawania pluginów?

Odpowiedź Zamawiającego:

Zamawiający dopuści takie rozwiązanie jako równoważne do wskazanego w Opisie przedmiotu zamówienia.

Pytanie 27:

Dotyczy C.20

System musi działać zarówno w trybie stand-alone jako dedykowany system analityczny jak i część większego systemu bezpieczeństwa działającego inline lub na kopii ruchu.

Czy zamawiający dopuści rozwiązanie pracujące na plikach przekazywanych do analizy zamiast inline?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy OPZ. Zamawiający planuje wykorzystanie systemu pracującego na kopii ruchu lub in-line. Skanowanie in-line zapewni ochronę w czasie rzeczywistym. Skanowanie plików zapewni jedynie zidentyfikowanie zagrożenia.

Pytanie 28:

Dotyczy C.21

W trybie stand-alone system musi umożliwiać zarządzanie oparte o role / RBAC, w tym minimum rola administratora systemowego, analityka, API i pełnego administratora.

Czy zamawiający dopuści rozwiązanie nie posiadające podziału na role, posiadające wewnętrzny interfejs do komunikacji z proponowanymi rozwiązaniami proxy?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy OPZ. Wymagany jest podział na role dla osób administrujących i obsługujących system. Ze względu na zapewnienie zgodności z polityką bezpieczeństwa, konieczny jest podział na role osób obsługujących system, zgodnie z zasadą najmniejszych koniecznych uprawnień.

Pytanie 29:

Dotyczy C.22

Każdy z użytkowników o odpowiednim poziomie uprawień musi mieć możliwość pisania własnych sygnatur złośliwych zachowań, ograniczając zakres ich obowiązywania, do plików które przez niego są detonowane.

Czy zamawiający dopuści rozwiązanie posiadające mechanizmy dynamicznej emulacji dowolnych wzorców zachowań i dynamicznego podstawiania dowolnego sprzętu i oprogramowania bez możliwości dodawania sygnatur dowolnych zachowań ?

Odpowiedź Zamawiającego:

Zamawiający dopuści takie rozwiązanie jako równoważne do wskazanego w Opisie przedmiotu zamówienia.

Pytanie 30:

Dotyczy C.23

Podczas procesu ręcznej detonacji system musi dawać możliwość określenia dodatkowych argumentów wykonania próbki i ścieżki w system w której ma się wykonać.

Czy zamawiający dopuści rozwiązanie posiadające mechanizmy dynamicznej emulacji dowolnych wzorców zachowań i dynamicznego podstawiania dowolnego sprzętu i oprogramowania bez możliwości dodawania sygnatur dowolnych próbek i ścieżki w systemie z której ma się wykonać?

Odpowiedź Zamawiającego:

Zamawiający podtrzymuje zapisy OPZ. Podczas procesu ręcznej detonacji system musi dawać możliwość określenia parametrów detonacji.

Pytanie 31:
Dotyczy C.27
Jednym ze źródeł reputacyjnych dla plików musi być serwis VirusTotal lub inny serwis o podobnej skali zastosowania pokazujący, ile i jakie silniki AV rozpoznają dany plik jako malware.
Czy zamawiający dopuści rozwiązanie nie posiadające obrazowania na portalach refutacyjnych firm trzecich tylko na sowim?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Wymagane jest użycie przez system powszechnie uznanych źródeł reputacyjnych oprócz wbudowanych w system. Umożliwi to zwiększenie wiarygodności uzyskiwanych wyników związanych z zagrożeniami.

Pytanie 32:
Dotyczy C.28
Wymagana jest możliwość eksportu wyników detonacji pliku w formacie STIX w celu dalszej analizy przez inne systemy.
Czy zamawiający odpuści rozwiązanie posiadające jedynie swój mechanizm do analizy malwale?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie jako równoważne do wskazanego w Opisie przedmiotu zamówienia, posiadające jedynie swój mechanizm do analizy malwale.

Pytanie 33:
Dotyczy C.31
System musi umożliwiać analizę dynamiczną każdego pliku, dla którego istnieje w systemie oprogramowanie go wykonujące, również po modyfikacji profili wirtualnych systemów.
Czy zamawiający dopuści rozwiązanie nie posiadające możliwości modyfikacji profili wirtualnych systemów?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. System musi umożliwiać analizę dynamiczną każdego pliku, dla których Zamawiający posiada oprogramowanie.

Pytanie 34:
Dotyczy C.34
System musi umożliwiać przeszukiwanie zbioru przenalizowanych plików min. w oparciu o hash MD5 lub SHA256 oraz Risk Score.
Czy zamawiający dopuści rozwiązanie posiadające tylko jeden z wymienionych algorytmów hash?
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Wymienione powyżej algorytmy są wykorzystywane przez Zamawiającego.

Pytanie 35:
Dotyczy C.36
Wymagana jest możliwość integracji z systemem ochrony poczty elektronicznej – obecnie Trend Micro InterScan Messaging Security Virtual Appliance.
Czy zamawiający dopuści rozwiązanie nie posiadające integracji z rozwiązaniami Ternd Micro. Integracja taka wskazuje na faworyzowanie jednego z dostawców i jest wbrew zasadom zachowania uczciwej konkurencji PZP.
Odpowiedź Zamawiającego:
Zamawiający podtrzymuje zapisy OPZ. Zamawiający posiada oprogramowanie Trend Micro InterScan Messaging Security Virtual Appliance i wymaga integracji systemu z tym oprogramowaniem.

Pytanie 36:
Dotyczy C.37
Wymagana minimalna ilość jednocześnie uruchomionych maszyn wirtualnych w systemie to 25.

Czy zamawiający dopuści rozwiązanie emulacyjne, gdzie minimalna ilość maszyn VM nie jest określona?
Odpowiedź Zamawiającego:
Zamawiający dopuści rozwiązanie emulacyjne, gdzie minimalna ilość maszyn VM nie jest określona. W przypadku wirtualizacji ilość maszyn wirtualnych musi być nie mniejsza niż 25.

Pytanie 37:
Dotyczy C.38
Każde z urządzeń musi mieć wydajność umożliwiającą przeprowadzenia analizy minimum 8000 próbek malware w ciągu 24h.
Czy zamawiający dopuści urządzenie posiadające możliwość analizy 10 000 próbek malware na dzień bez określania ich wielkości ani typu pliku, tj. malware o wielkości 1kb w pliku tekstowym wykażą bardzo dużą przepustowość systemu. Czy zamawiający w związku z powyższym dopuści dowolne rozwiązanie posiadające dowolną przepustowość?
Odpowiedź Zamawiającego:
Zamawiający dopuszcza rozwiązania zgodne z OPZ, umożliwiające analizę minimum 8000 próbek malware w ciągu 24 godzin przy zachowaniu wszystkich wymagań OPZ.

Przewodniczący
Komisji Przetargowej
Bartosz Wielądek
Konsultant
w Wydziale zamówień Publicznych GUS