PYTANIA I ODPOWIEDZI			
Nr pytania	**Referencja do RFI**	**Treść Pytania**	**Odpowiedź EITE**
1.	pkt. 2.4	Czy wymagane szkolenia mają być szkoleniami producenta rozwiązania czy szkolenia autorskie przeprowadzone przez parntera spersonalizowane pod kątem wdrożonych u Zamawiającego rozwiązań uwzględniające ścieżkę szokleniową producenta?	Zamawiający dopuszcza szkolenia autorskie, jeżeli swoim zakresem obejmują obszary analogiczne do szkoleń autoryzowanych.
2.	pkt. 2.4	Czy szkolenia mają się odbywać w siedzibie Zamawiającego czy w innych lokalizacjach, zdalnie?	Zamawiający nie określa miejsca realizacji szkoleń wstępnych, niemniej szkolenie z wykorzystaniem funkcjonującego u Zamawiającego Rozwiązania należy rozważyć w miejscu wskazanym przez Zamawiajacego
3.	pkt. 2.4	Czy szkolenie dla analityków bezpieczeństwa będzie się odbywało dla 10 osób czy liczba tych osób będzie przez Zamawiającego podzielona np. na dwie grupy po 5 osób?	Zamawiający zakłada podział na dwie grupy po 5 osób.
4.	2.	Czy zamawiający dopuszcza, by w ramach przetargu oprogramowanie antywirusowe zostało dostarczone wraz z rozwiązaniem Advanced Threat Protection (sandbox)?	Zakup oprogramowania antywirusowego nie jest przedmiotem powyższego postępowania.
5.	6.	Czy zamawiający dopuszcza rozwiązanie, które będzie posiadać możliwość poszukiwania urządzeń wykazujących się konkretnymi cechami (w tym m.in. uruchomienie aplikacji, wykorzystanie biblioteki DLL, uruchomienie skryptu, czy też zastosowanie argumentów w wierszu poleceń)?	Tak, Zamawiający prosi jednak o zwrócenie uwagi, że produkt musi być zgodny z Opisem Przedmiotu Zamówienia (OPZ).
6.	7.	Czy zamawiający dopuszcza rozwiązanie, które będzie posiadać możliwość zdalnej remediacji zagrożenia, poprzez terminowanie procesów, usuwanie plików i zmian w rejestrach za pomocą linii komend? Rozwiązanie pokazuje zachowanie procesu w systemie, pokazując zmiany w rejestrze systemowym?	Tak, Zamawiający prosi jednak o zrwócenie uwagi, że produkt musi być zgodny z OPZ.
7.	8.	Czy zamawiający dopuszcza rozwiązanie, które będzie komunikowało się za pomocą agenta do serwera co kilka minut, przesyłając informacje na bieżąco. Dodatkowo rozwiązanie posiada funkcję wymuszenia podłączenia agenta - tzw. sygnał wznowienia, który umożliwia natychmiastowe podłączenie danego agenta	Tak, Zamawiający prosi jednak o zrwócenie uwagi, że produkt musi być zgodny z OPZ.
8.	9.	Czy zamawiający dopuszcza rozwiązanie, którego część rozwiązania EDR, cała część AV oraz część związana z Sandbox będzie zarządzana z poziomu jednej konsoli, natomiast bardziej zaawansowane funkcje EDR będą dostępne w drugiej konsoli. Istnieje możliwość przełączania się między konsolami za pomocą odnośników - z pierwszej konsoli do drugiej i odwrotnie.	Tak, Zamawiający dopuszcza zmianę konsoli w przypadku przełączania za pomoca odnośników.
9.	10.	Czy zamawiający dopuszcza rozwiązanie, które pozwala na przesłanie artefaktów do systemu SIEM lub syslog?	Zamawiający oczekuje informacji o zdarzeniu w systemie SIEM. Zamawiający nie dopuszcza wysyłania do systemu SIEM artefaktów w postaci zainfekowanych plików i tym podobnych.
10.	13.	Czy zamawiający dopuszcza rozwiązanie, które w pełni wspiera systemy Desktop od wersji 7 wzwyż oraz systemy Windows Server od wersji 2008 R2 SP1 wzwyż?	Zamawiający prosi o zaznaczenie w informacji o produkcie tego faktu.
11.	14.	Czy zamawiający dopuszcza rozwiązanie, które dla systemów Linux będzie dawało możliwość tylko zainstalowania systemu antywirusowego, który będzie chronił przed wszelkiego rodzaju zagrożeniami?	Zakup oprogramowania antywirusowego nie jest przedmiotem powyższego postępowania.

12.	21.	Czy zamawiający dopuszcza rozwiązanie, które w przypadku zagrożenia da możliwość przeanalizowania skąd się wzięło zagrożenie, z jakimi serwerami się łączyło oraz jakie pliki wykonywalne zostały zrzucone dla danego procesu z możliwością weryfikacji w jaki sposób zagrożenie zostało w systemie uruchomione, bez budowania mapy?	Tak, jeżeli informacja dostarczona przez Rozwiązanie pozwala na jednoznaczną identyfikację całości przebiegu zdarzenia.
13.	26.	Czy zamawiający dopuszcza rozwiązanie, w którym zdarzenia będą wywoływać alarmy, a te będą powiązane z bazą Mitre Att&ck, dzięki czemu każdy alarm będzie posiadał wyjaśnienie oraz sugerowane rozwiązanie zdarzenia.	Tak
14.	27.	Czy zamawiający dopuszcza rozwiązanie, które będzie w przypadku utraty komunikacji z systemami aktualizacji Producenta pod kątem antywirusowym, a także EDR działało z ostatnimi aktualizacjami modułów, a w przypadku rozwiązania typu Sandbox, rozwiązanie zacznie działać po przywróceniu komunikacji?	Tak
15.	28.	Czy zamawiający dopuszcza rozwiązanie, które posiada globalną reputację plików, a lokalną można potraktować jako popularność (ilość wystąpień) pliku w sieci zamawiającego?	Tak
16.	32.	Czy zamawiający dopuszcza rozwiązanie, które posiada opcję ręcznego wywołania analizy próbki tylko dla pliku w sandbox? URL może być weryfikowany za pomocą modułów antywirusowych	Zamawiający oczekuje możliwości wywołania analizy w Rozwiązaniu dla każdego zidentyfikowanego potencjalnego artefaktu
17.	33.	Czy zamawiający dopuszcza rozwiązanie, które pokaże po detonacji potencjalnie szkodliwe i nieszkodliwe działanie oraz skrót SHA-1, które pozwoli na znalezienie tego pliku w rozwiązaniu EDR, w celu podglądu na jakich stacjach został plik uruchomiony, z jakiej aplikacji pochodzi, jaki był adres URL połączenia, jakie zostały zrzucone pliki wykonywalne, itp.?	Tak
18.	34.	Czy zamawiający dopuszcza rozwiązanie, które automatycznie dostosowuje środowisko sandbox do środowiska produkcyjnego zamawiającego?	Tak
19.	37, 38, 39.	Czy zamawiający dopuszcza rozwiązanie, które może zostać uruchomione on-premise w wersji fizycznej lub wirtualnej, a sandbox będzie rozwiązaniem chmurowym ze spełnieniem wszystkich wymagań przetrzymywania danych na terenie Unii europejskiej (serwer w UE), wraz z możliwością usunięcia pliku natychmiast po analizie?	Zamawiający nie dopuszcza użycia rozwiązań chmurowych jako cześci Rozwiązania
20.	3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP), punkt 13.	Czy zamawiający dopuszcza wsparcie dla platform serwerowych od Windows 2008R2 zamiast od Windows 2003 R2 (którego EoL był w połowie 2015 roku)?	Zamawiający prosi o zaznaczenie w informacji o produkcie tego faktu.
21.	3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP), punkt 29	Czy rozwiązanie ma działać w oparciu konkretnie o czarne i białe listy na podstawie sum kontrolnych, czy może realizować daną funkcjonalność w inny sposób (blacklist w formie compliance, whitelist jako wyjątki)?	Zamawiający, z uwagi na odmienną realizację tej funkcjonalności przez różne Rozwiązania, nie wskazuje sposobu realiacji.
22.	3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP), punkt 30	Czy zamawiający dopuszcza możliwość wykorzystania autorskiej bazy producenta w celu sprawdzenia zagrożenia?	Tak
23.	3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP), punkt 32	Prosimy o doprecyzowanie: co oznacza ręczne wywołanie analizy próbki URL? Wskazuje konkretny plik, pobranie jego i weryfikację?	Zamawiający jako ręczne wywołanie analizy próbki URL uznaje możliwośc weryfikacji bezpieczeństwa danego URL. Zamawiający, z uwagi na odmienną realizację tej funkcjonalności przez różne Rozwiązania, nie wskazuje sposobu realiacji.

24.	3. WYMAGANIA DLA ROZWIĄZANIA KLASY ADVANCED THREAT PROTECTION (ATP), punkt 34	Czy zamawiający dopuszcza stosowania tylko gotowych i sprawdzonych obrazów od producenta? Stosowanie obrazów ogólnych zapewnia zdecydowanie dużo wyższą wykrywalność niż zmieniane i modyfikowane obrazy (custom VM).	Tak
25.	3.2 „rozwiązanie musi zapewniać możliwość integracji z wykorzystywanym oprogramowaniem antywirusowym na stacjach roboczych i serwerach,"	Czy powyższe wymaganie określa, że dostarczone rozwiązanie ma współdziałać na stacjach roboczych i serwerach razem z wykorzystywanym oprogramowaniem antywirusowym bez zakłóceń? Czy możliwość integracji polega na czymś innym?	Zamawiajacy jako minimum oczekuje zdolności Rozwiązania do koegzystencji z oprogramowaniem antywirusowym na osłanianej platformie.
26.	3.9 „rozwiązanie musi być zarządzane z poziomu jednej konsoli,"	Mając na uwadze że zarządzenie poszczególnymi elementami rozwiązania ATP posiadają różne charakterystyki działania oraz w kontekście rozdzielności np. warstwy zarządzania od warststwy logowania i raportowania, czy zamawiajacy dopuści rozwiązania zarządzane z więcej niż jednej konsoli?	Nie, OPZ definiuje jednoznacznie wymaganie. Zamawiający dopuści więcej niż jedną konsolę w przypadku kierowania do innej konsoli poprzez bezpośrednie odnośniki.
27.	pkt. 3.13 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.	Czy dla starszych wersji systemów operacyjnych Microsoft zamawiający dopuści rozwiązane obsługujące te platformy zrealizowane w oparciu o starszą wersję agenta oferowanego rozwiązania ATP? W takim wypadku oferowane rozwiązanie zapewni wsparcie dla najstarszych wersji np. Windows Serwer 2003 R2 do momentu utrzymania wsparcia serwisowego określonej wersji agenta przez producenta rozwiązania ATP. Microsoft zaprzestał świadczenia wsparcia dla platformy Windows Serwer 2003 R2 14 lipca 2015 roku, tj. prawie 5 lat temu, trudno zatem oczekiwać pełnego wsparcia dla nierozwijanego oraz niewspieranego przez producenta systemu na nowoczesnym rozwiązaniu klasy ATP przez okres kolejnych 36 miesięcy od daty zakończenia wdrożenia takiego rozwiązania.	Tak