

PYTANIA I ODPOWIEDZI

Nr pytania	Referencja do RFI	Treść Pytania	Odpowiedź EITE
1.	pkt. 3.3 - rozwiązanie musi posiadać mechanizmy wykrywania zaawansowanych zagrożeń w kanale sieciowym.	Czy zamawiający wymaga dostarczenia urządzeń/oprogramowania dedykowanego do monitorowania kanału sieciowego? Jeśli tak to prosimy o podanie ilości oraz orientacyjnej przepustowości łącz, które sondy te mają monitorować.	<p>Zamawiający dopuszcza odseparowane rozwiązanie analizujące strumień ruchu sieciowego, proszę jednak pamiętać o zapisach RFI mówiących o możliwości zarządzania / analizy z poziomu jednej konsoli (rozwiązanie musiałoby pozwolić na integrację ze wskazanym, odseparowanym oprogramowaniem analizującym ruch sieciowy).</p> <p>Zamawiający nie precyzował szczegółowo mechanizmów wykrywania zagrożeń, ponieważ różne rozwiązania ATP realizują odmiennie podobne zadania. Zamawiający oczekuje jednak możliwości wykrycia w ruchu sieciowym anomalii generowanych przez host lub otoczenie, wykrywanych na bazie bądź to sygnatur/wzorców zachowania bądź też nietypowych aktywności (skanowanie), lub też innych, niewymienionych mechanizmów.</p> <p>Na tym etapie postępowania informacje dotyczące ilości oraz przepustowości łącz w infrastrukturze Zamawiającego nie mogą być udostępnione z uwagi na brak umowy NDA</p>
2.	pkt. 3.15 - rozwiązanie powinno umożliwiać budowę środowiska HA lub rozwiązanie musi zapewniać możliwość odtworzenia funkcjonalności po awarii oprogramowania w czasie nie dłuższym niż 4godziny, bez utraty danych historycznych i raportowych.	Jakie wymagania niezawodnościowe (HA) istnieją dla urządzeń do analizy złośliwego oprogramowania (sandbox)? Czy Zamawiający wymaga dostarczenia pary nadmiarowej takich urządzeń? Czy wystarczy zapewnienie możliwości odtworzenia funkcjonalności w czasie nie dłuższym niż 4h po awarii (dla pojedynczego urządzenia)?	Zamawiający nie wymaga nadmiarowości urządzeń do analizy złośliwego oprogramowania (sandbox). W tym zakresie wystarczy zapewnienie możliwości odtworzenia funkcjonalności w czasie nie dłuższym niż wskazany w RFI (dla pojedynczego urządzenia).