

Opis Przedmiotu Zamówienia (OPZ)

I. PRZEDMIOT ZAMÓWIENIA

Przedmiotem Zamówienia jest zakup rozbudowa posiadanego środowiska Trend Micro Vision One o moduł zaawansowanej ochrony kanału pocztowego.

1. 12000 subskrypcji oprogramowania.
2. wdrożenie funkcjonalności w środowisku IT Zamawiającego.
3. usługi wsparcia technicznego na okres 36 miesięcy.

II. Subskrypcje oprogramowania muszą zapewnić co najmniej niżej opisane wymagania:

Kategoria funkcjonalności	Funkcjonalność
Informacje ogólne	<p>Rozwiązanie musi zapewniać ochronę usługi Microsoft Exchange Online pracującej w modelu hybrydowym, gdzie skrzynki pocztowe znajdują się zarówno w chmurze jak i lokalnej infrastrukturze IT Zamawiającego. Oferowane rozwiązanie musi zarówno wykonać analizę wiadomości email poprzez bezpośrednie podpięcie do skrzynki pocztowej znajdującej się w chmurze Microsoft jak i musi wykonywać analizę poprzez integrację z Microsoft Exchange Online w trybie inline umożliwiającą analizowanie poczty znajdującej się na skrzynkach on-prem. Integracja z Microsoft Exchange w trybie inline musi odbywać się poprzez wykreowanie dedykowanej aplikacji w usłudze Microsoft Online i integrację z Entra ID. Integracja ze środowiskiem Microsoft Exchange Online nie może wymagać modyfikacji rekordów MX DNS.</p> <p>Rozwiązanie również musi zapewniać ochronę co najmniej następujących usług Microsoft 365: Exchange online, Onedrive, SharePoint Online, Microsoft Teams, Microsoft Teams Chat.</p> <p>Rozwiązanie musi być dostarczone w formie SaaS i w całości ma być zarządzane z poziomu centralnej konsoli zarządzającej Trend Vision One.</p>

Kategoria funkcjonalności	Funkcjonalność
Wymagania funkcjonalne rozwiązania	<p>Musi dostarczać ochronę przed zaawansowanymi zagrożeniami ATP (Advanced Threat Protection) dla następujących usług:</p> <ul style="list-style-type: none"> • OneDrive • MS SharePoint Online • MS Teams (chat) <p>MS Exchange Online poprzez:</p> <ul style="list-style-type: none"> • Integrację za pomocą API i analizę zagrożeń bezpośrednio poprzez podpięcie do chronionych skrzynek pocztowych znajdujących się w chmurze Microsoft • in-line poprzez wykreowanie dedykowanej aplikacji w usłudze Microsoft Online i integrację z Entra ID. <p>Integracja ze środowiskiem Microsoft Exchange Online nie może wymagać modyfikacji rekordów DNS, a rozwiązanie nie może działać jako klasyczne MTA.</p> <p>Niezależnie od objętej ochroną usługi (OneDrive, Sharepoint, Teams, Exchange) rozwiązanie musi pozwalać na wykonanie zaawansowanej analizy plików w środowisku sandbox oraz adresów URL.</p> <p>Musi zapewnić sandboxing w chmurze do automatycznej detekcji i analizy potencjalnie złośliwych załączników oraz adresów URL w bezpiecznym środowisku wirtualnym hostowanym przez producenta</p> <ul style="list-style-type: none"> • Średni czas analizy próbek w środowisku sandbox powinien nie przekraczać 3 min • Przed podjęciem decyzji o przestaniu próbki do analizy w środowisku sandbox system musi wykonać jej analizę wykorzystując zaawansowane symulacje działań złośliwych w czasie zbliżonym do rzeczywistego <p>Po zakończeniu analizy próbki w środowisku sandbox musi zostać wygenerowany szczegółowy raport, który będzie zawierał:</p> <ul style="list-style-type: none"> • Typ pliku, nazwę, rozmiar oraz skróty: SHA-1 i MD5 • Podsumowanie złośliwych cech, z podziałem na odpowiednie kategorie • Ocenę ryzyka – niskie, średnie, wysokie – możliwość zdefiniowania akcji, którą system podejmie po wykryciu próbki o danym ryzyku • Szczegóły zachowania próbki w testowanym systemie: • Lista adresów i domen użytych w komunikacji sieciowej, wraz z oceną ich ryzyka • Lista otwartych portów, na których próbka nasłuchuje • Szczegóły zidentyfikowanego kanału komunikacji C&C • Lista tworzonych lub pobranych plików wraz z wynikiem ich analizy • Lista tworzonych procesów <p>Musi wykorzystywać usługę reputacji sieciowej do analizy i blokowania adresów URL, w szczególności musi wykorzystywać:</p> <ul style="list-style-type: none"> • Statyczną listę reputacji z możliwością dostrojenia czułości działania (np. najmniej agresywne, średnio agresywne, agresywne) • Dynamiczne skanowanie URL – dla nieznanymi, nieistniejących jeszcze w bazie statycznych adresów • Analizę przy użyciu algorytmów widzenia komputerowego, pozwalająca wykryć i zablokować przypadki phishingu (wyłudzenia poświadczeń dla serwisów Microsoft'u) <p>Usługa reputacji ma umożliwiać analizę adresów URL pochodzących z treści wiadomości a także z plików wymienianych jako załączniki przez OneDrive, Sharepoint i chat Teams</p>

	<p>Ochrona anty-spamowa dla Exchange Online:</p> <ul style="list-style-type: none"> • Musi umożliwiać zdefiniowania poziomu czułości mechanizmów ochrony (najmniej agresywna, średnio agresywna, agresywna) • Musi wykrywać i blokować wiadomości typu gray-mail, w tym na przykład newsletterów, powiadomień z sieci społecznościowych, forów • Musi oferować ochronę przed atakami BEC – Business Email Compromise – dedykowany silnik analizujący nagłówki oraz treść korespondencji • Musi umożliwiać zdefiniowania użytkowników typu VIP oraz ważnych domen dla silnika BEC, wykrywanie ataków podszywania się z użyciem bliźniaczych domen oraz nadawców • Musi umożliwiać dodanie wyjątków na podstawie nagłówka wiadomości lub adresów oraz domen nadawców • Musi umożliwiać ręczne zablokowania nadawcy lub domeny <p>Rozwiązanie musi posiadać mechanizm ochrony przed wyciekiem danych (DLP) dla OneDrive, Teams oraz Sharepoint, umożliwiający co najmniej:</p> <ul style="list-style-type: none"> • Blokowanie na podstawie predefiniowanych wzorców • Definiowanie własnych identyfikatorów danych z użyciem wyrażeń regularnych (regex) • Tworzenie reguł, z wykorzystaniem własnych oraz wbudowanych list słów kluczowych i identyfikatorów danych • Wykorzystania reguł DLP do monitorowania także ruchu poczty elektronicznej • Posiadający wbudowane polskie identyfikatory ochrony danych, przynajmniej dla: • Pesel • Numer Dowodu Osobistego • Numer rachunku bankowego • Numer telefonu • Blokowanie na podstawie listy statycznej słów kluczowych <p>Rozwiązanie musi umożliwiać skonfigurowanie akcji jaka zostanie podjęta po wykryciu zagrożeń, w oparciu o ich kategorię:</p> <ul style="list-style-type: none"> • Kwarantanna (musi być zintegrowana ze środowiskiem MS365 Zamawiającego) • Kasowanie • Przepuszczenie • Dla wiadomości email dodatkowo: ostemplowanie treści lub tematu, przeniesienie do folderu wiadomości-śmieci
--	---