Transportowy Dozór Techniczny
ul. Puławska 125
02-707 Warszawa
tel.: +48 22 490 29 02
e-mail: info@tdt.gov.pl

niepodległa | POLSKA STULECIE ODZYSKANIA NIEPODLEGŁOŚCI

Warszawa, dn. 23.08.2021 r.

Wykonawcy
Nr referencyjny postępowania ZP 7/2021

Znak sprawy: P.290.3.2021.PZ
dotyczy: postępowania o udzielenie zamówienia publicznego: Dostawa sprzętu sieciowego, Nr referencyjny postępowania: ZP 7/2021.

INFORMACJA Z OTWARCIA OFERT

Transportowy Dozór Techniczny działając jako Zamawiający zgodnie z przepisami art. 222 ust. 5 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (Dz. U. z 2021 r. poz. 1129 ze zm.), zawiadamia, iż w dniu 23 sierpnia 2021 r. o godzinie 11.00 za pośrednictwem miniPortalu odbyło się otwarcie ofert w niniejszym postępowaniu. W terminie przewidzianym na składanie ofert, tj. do dnia 23 sierpnia 2021 r. do godz. 9:00 wpłynęły dwie oferty:

Lp.	Nazwa lub imię i nazwisko, siedziba lub miejsce prowadzenia działalności gospdarczej albo miejsce zamieszkania Wykonawcy	Cena zawarta w ofercie (zł)	Oferowana funkcjonalność	Wybór
1	ComCERT SA Warszawa	**2 458 798,49**	Urządzenie firewall posiada funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach anty-wirus oraz funkcji filtrowania URL pozwalając jednocześnie znacznie zmniejszyć okres ryzyka dla pacjenta ZERO. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych: - złośliwych plików wykonywalnych (tzw. PE i DLL) - złośliwych skryptów PowerShell - złośliwych stron / ataków Phishing - złośliwych skryptów JavaScript	x
			Urządzenie posiada koncept konfiguracji kandydackiej (na poziomie API, GUI oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. W tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji	x
			Urządzenie umożliwia sprawdzenie wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w GUI urządzenia firewall i nie może wymagać korzystania z rozwiązań trzecich.	x
2	Netsecure Sp. z o. o. Warszawa	**1 383 750,00**	Urządzenie firewall posiada funkcjonalność blokowania zagrożeń za pomocą algorytmów uczenia maszynowego (ML) aktualizowanych dynamicznie przez producenta. Wykrywanie za pomocą algorytmów musi odbywać się lokalnie na urządzeniu jako uzupełnienie posiadanych funkcji bazujących na sygnaturach anty-wirus oraz funkcji filtrowania URL pozwalając jednocześnie	x

Lp.	Nazwa lub imię i nazwisko, siedziba lub miejsce prowadzenia działalności gospdarczej albo miejsce zamieszkania Wykonawcy	Cena zawarta w ofercie (zł)	Oferowana funkcjonalność	Wybór
			znacznie zmniejszyć okres ryzyka dla pacjenta ZERO. Wymagane jest posiadanie funkcji wykrywania za pomocą ML (Machine Learning) dla następujących danych: - złośliwych plików wykonywalnych (tzw. PE i DLL) - złośliwych skryptów PowerShell - złośliwych stron / ataków Phishing - złośliwych skryptów JavaScript	
			Urządzenie posiada koncept konfiguracji kandydackiej (na poziomie API, GUI oraz CLI), którą można dowolnie edytować na urządzeniu bez automatycznego zatwierdzania wprowadzonych zmian w konfiguracji urządzenia do momentu, gdy zmiany zostaną zaakceptowane i sprawdzone przez administratora systemu. W tym: a. Możliwość edytowania konfiguracji kandydackiej przez wielu administratorów pracujących jednocześnie i pozwalać im na zatwierdzanie i cofanie zmian, których są autorami. b. Możliwość blokowania wprowadzania i zatwierdzania zmian w konfiguracji systemu przez innych administratorów w momencie edycji konfiguracji	X
			Urządzenie umożliwia sprawdzenie wpływu nowo pobranych aktualizacji sygnatur wykrywających aplikacje (przed ich zatwierdzeniem na urządzeniu) na istniejące polityki bezpieczeństwa – funkcja ta musi być wbudowana w GUI urządzenia firewall i nie może wymagać korzystania z rozwiązań trzecich.	X