BIŁ.2233.23.2024.PB

Załącznik nr 1 do

Wniosku o udzielenie zamówienia

**Opis przedmiotu zamówienia**

**1. Przedmiot Zamówienia**

Zakup licencji na skaner podatności dla 300 urządzeń na okres 24 miesięcy.

**2. Wymagania Funkcjonalne i Techniczne Skanera Podatności**

* **Identyfikacja Podatności**: Narzędzie musi umożliwiać identyfikację i analizę podatności na poziomie systemów operacyjnych, aplikacji oraz urządzeń sieciowych.
* **Aktualna Baza Podatności**: Baza musi być regularnie aktualizowana i obejmować znane podatności (np. CVE) oraz inne luki bezpieczeństwa.
* **Skanowanie Autoryzowane i Nieautoryzowane**: Narzędzie powinno umożliwiać zarówno skanowanie autoryzowane (przy wykorzystaniu danych uwierzytelniających), jak i nieautoryzowane.
* **Elastyczność Trybów Skanowania**: Możliwość wykonywania pełnych skanów, skanów przyrostowych, skanów aplikacji webowych oraz szybkich skanów wybranych zasobów.
* **Audyt Zgodności**: Wsparcie dla audytów zgodności z wytycznymi i regulacjami (np. PCI-DSS, HIPAA, GDPR).

**3. Wymagania Integracji**

* **Integracja z Trellix XDR**: Narzędzie musi wspierać integrację z platformą Trellix XDR, zarówno dla wersji on-premise, jak i cloud, aby zapewnić centralizację danych o podatnościach oraz ich zarządzanie.
* **API**: Wymagana jest dostępność API, które pozwoli na integrację z zewnętrznymi narzędziami do zarządzania incydentami bezpieczeństwa, systemami zarządzania ryzykiem (SIEM, CMDB), a także do automatyzacji działań naprawczych.

**4. Wymagania Wydajnościowe i Skalowalność**

* **Obsługa do 300 Urządzeń**: Licencja powinna obejmować minimum 300 urządzeń z możliwością skalowalności.
* **Wiele Sesji Równoległych**: Możliwość równoczesnego skanowania w wielu sesjach, bez wpływu na wydajność narzędzia.

**5. Wymagania Bezpieczeństwa**

* **Zabezpieczenia Dostępu**: Autoryzacja i uwierzytelnianie użytkowników (np. integracja z LDAP/Active Directory).
* **Logowanie i Audyt**: Funkcje logowania zdarzeń oraz audytowania dostępu i działań w narzędziu.
* **Szyfrowanie Komunikacji**: Szyfrowanie komunikacji między komponentami narzędzia (np. podczas przesyłania danych między agentami i serwerem).

**6. Wymagania Dotyczące Raportowania i Analizy**

* **Raportowanie Podatności**: Narzędzie powinno generować szczegółowe raporty obejmujące wyniki skanowania, analizę ryzyka i rekomendacje naprawcze.
* **Dostosowanie Raportów**: Możliwość tworzenia raportów dostosowanych do potrzeb różnych grup odbiorców.
* **Priorytetyzacja Podatności**: Narzędzie musi umożliwiać klasyfikację podatności na podstawie krytyczności, aby ułatwić priorytetyzację działań naprawczych.

**7. Wdrożenie i Konfiguracja**

* **Usługa Wdrożenia**: Wykonawca zapewni pełne wdrożenie, konfigurację i dostosowanie narzędzia do środowiska zamawiającego nie później, niż do dnia 18.12.2024 r.
* **Szkolenie Użytkowników**: Przeprowadzenie szkolenia dla administratorów.
* **Testy i Walidacja**: Wykonanie testowych skanów w celu weryfikacji wyników i dopasowania konfiguracji do środowiska zamawiającego.

**8. Wsparcie Techniczne**

* **Wsparcie na Okres Licencji**: Gwarancja wsparcia technicznego przez 24 miesiące, dostępność wsparcia 24/7 (w języku polskim lub angielskim).
* **Pomoc w Rozwiązywaniu Problemów**: Możliwość kontaktu w celu zgłaszania incydentów, rozwiązywania problemów oraz konsultacji technicznych.