Opis Przedmiotu Zamówienia

1. Prawa własności dotyczące zamawianej aplikacji

2. Przedmiotem zamówienia jest wytworzenie aplikacji desktopowej na system operacyjny Windows i przekazanie Zamawiającemu wyłącznych praw do wytworzonej aplikacji.
3. Wyłączne prawa przekazywane Zamawiającemu dotyczą jedynie samej aplikacji; jeśli do poprawnego działania aplikacji niezbędne będzie oprogramowanie antywirusowe zainstalowane lokalnie na tym samym komputerze, co działająca aplikacja – Zamawiający nie wymaga przeniesienia na siebie praw własności oprogramowania antywirusowego.
4. Zamawiający planuje udzielenie Wykonawcy tzw. Licencji zwrotnej, czyli udzieleniu praw umożliwiających dalsze rozwijanie aplikacji we własnym zakresie w celu jej komercjalizacji.

2. Główna funkcjonalność zamawianej aplikacji

1. Aplikacja musi realizować funkcjonalność sanityzacji zewnętrznych nośników danych.
2. Przez pojęcie sanityzacji Zamawiający rozumie dokonanie akcji skanowania antywirusowego i/lub dokonania symulacji zachowania pliku w wyizolowanym wirtualnym środowisku na plikach znajdujących się na zewnętrznym nośniku i zwrócenie komunikatu o braku/ilości istniejących zagrożeń, zostawiając użytkownikowi autonomię w decyzji reakcji na zagrożenie.
3. Zamawiającemu zależy na jak najbardziej wiarygodnym wyniku procesu sanityzacji. W tym celu Zamawiający wymaga implementacji logiki decydującej o tym, jakie pliki wystarczy skanować lokalnie, a jakie pliki należy przeanalizować z wykorzystaniem Sandbox'a zlokalizowanego w infrastrukturze sieciowej Resortu Sprawiedliwości.
4. Implementacja logiki decyzyjnej opisanej w powyższym punkcie będzie przedmiotem konkursu przewidzianego w art. 110 ustawy Prawo zamówień publicznych, jaki Zamawiający planuje zorganizować w celu wyłonienia twórcy potencjalnie najlepszego rozwiązania. Kryteria według których oceniane będą prace konkursowe to: szybkość uzyskiwanych wyników skanowania, a także precyzja w określeniu wyniku skanowania.
5. Jeśli w toku konkursu, o którym mowa w punkcie powyższym okaże się, że skanowanie lokalne nie ma znaczącego wpływu na poprawę szybkości i/lub precyzji otrzymywanych wyników -Zamawiający dopuszcza sytuację, w której Wykonawca zrezygnuje ze skanowania lokalnego.
6. W przypadku wykorzystania lokalnego oprogramowania antywirusowego – Zamawiający oczekuje, że to Wykonawca dokona wyboru i zakupu oprogramowania antywirusowego na potrzeby działania aplikacji, a następnie dostarczy je w wersji instalacyjnej, z bazą sygnatur aktualnych na dzień nie starszy niż miesiąc, licząc od daty podpisania umowy.
7. W celu dokonania symulacji zachowania pliku w wyizolowanym wirtualnym środowisku Zamawiający udostępnia do wykorzystania Sandbox Trend Micro, znajdujący się w infrastrukturze sieciowej Resortu Sprawiedliwości. Zamawiający nie dopuszcza możliwości przesyłania sanityzowanych plików poza infrastrukturę Zamawiającego, np. w celu skorzystania z Sandboxów zewnętrznych dostawców.
8. Aplikacja musi umożliwiać następujące opcje działania w reakcji na wykryte zagrożenie: jedynie poinformowanie o wykrytym potencjalnym zagrożeniu, skopiowanie na inny zewnętrzny nośnik jedynie tych plików, jakie aplikacja uznała za bezpieczne lub wysyłka domenową pocztą elektroniczną wybranych plików, które zostały uznane przez aplikację za bezpieczne.

3. Pozostałe funkcjonalności zamawianej aplikacji

1. Zamawiający wymaga także integracji z Active Directory, m.in. w celu zrealizowania funkcjonalności integracji rozwiązania z pocztą elektroniczną organizacji.
2. Oprogramowanie musi umożliwiać funkcję integracji z oprogramowaniem typu SIEM, np. wystawiając API REST, tak aby aplikacja mogła zostać wykorzystana jako źródło logów - stanowiącej wkład do wiedzy o zagrożeniach pojawiających się w organizacji.
3. Oprogramowanie musi realizować – np. za pomocą zrealizowanej integracji z oprogramowaniem typu SIEM - funkcję centralnego logowania informacji o przeskanowanych nośników.
4. Logowane muszę być następujące informacje: dane dotyczące znalezionych zagrożeń, ich typów, czasu i lokalizacji zdarzeń. Jako lokalizację zdarzeń można przyjąć nazwę użytkownika w AD, a w przypadku konta „gość" identyfikator kiosku, na którym wystąpiło zdarzenie. Ponadto Zamawiający wymaga, aby gromadzone były dane pozwalające stwierdzić jakie konkretnie pliki były skanowane: tak, aby móc potwierdzić fakt skanowania nośnika przez pracownika. W opinii Zamawiającego wystarczające będą sumy kontrolne, tzw. hashe skanowanych plików wraz z numerem seryjnym podłączanego nośnika.
5. Aplikacja musi umożliwiać obsługę nośników zaszyfrowanych programem Bitlocker. Obsługa taka musi polegać na opcji odszyfrowania nośnika pod warunkiem podania przez przez użytkownika poprawnego hasła do nośnika.
6. Aplikacja musi także umożliwiać obsługę archiwów popularnych formatów archiwów danych: .rar, .zip, .tar, .7z, itp.
7. W przypadku archiwów niezaszyfrowanych domyślnym działaniem aplikacji powinno być rozpakowanie i analiza treści plików. Jednak nie dotyczy to sytuacji, w której użytkownik wcześniej wykluczy dany folder/archiwum z zakresu analizy. W przypadku archiwów zabezpieczonych hasłem aplikacja powinna wyświetlać komunikat z zapytaniem o hasło i/lub opcją pominięcia archiwum.
8. Aplikacja musi oferować użytkownikowi możliwość dokonania wstępnej selekcji folderów i plików, których proces w ogóle ma dotyczyć (w szczególności możliwość wykluczenia plików, których nie należy skanować). Wybór powinien dotyczyć zarówno poszczególnych plików jak i całościowo, dla wszystkich plików danego rozszerzenia (np.: pominięcie plików .vbs, .exe itp.)
9. Zamawiający dopuszcza możliwość udostępniania Wykonawcy logów debuggowych, pod warunkiem że logi te będą zanonimizowane, tj. nie będą zawierać danych osobowych (np. nazw stacji roboczych), nie będą zawierać analizowanych plików, ani innych informacji szczątkowych, których wyciek mógłby prowadzić do odtworzenia tajemnicy zawodowej – treści analizowanych pism, metadanych wskazujących na pochodzenie pliku itp.
10. Aplikacja musi posiadać dwa tryby pracy – tryb desktopowy oraz tryb kiosku.
11. Jako tryb kiosku Zamawiający rozumie takie przystosowanie aplikacji, aby uniemożliwić użytkownikowi komputera z uruchomioną w trybie kiosku aplikacją wykorzystanie go w celu realizacji jakiejkolwiek innej funkcjonalności niż tych oferowanych przez aplikację. Wyjście z trybu kiosku musi być chronione hasłem.
12. Jako tryb desktopowy Zamawiający rozumie takie działanie aplikacji, które nie koliduje z korzystaniem z innych funkcjonalności komputera, na którym aplikacja jest uruchomiona. Innymi słowy, jest to tryb w którym aplikacja działa w odrębnym oknie, umożliwiając jej minimalizowanie i symultaniczną pracę z innymi aplikacjami.