

Opis przedmiotu zamówienia

Przedmiot zamówienia: **Dostawa systemu typu sandbox**

Zamówienie obejmuje dostawę Systemu typu sandbox (zwanego dalej „Systemem”) służącemu ochronie przed atakami typu APT (Advanced Persistent Threat) będącego rozszerzeniem funkcjonalności używanego przez Zamawiającego systemu Secure Mail Gateway FortiMail wraz z wdrożeniem, gwarancją oraz instruktażem stanowiskowym.

1. Wymagania dla Systemu:

- 1.1. System powinien zostać dostarczony w formie virtual appliance uruchomionej w środowisku Zamawiającego.
- 1.2. Dostarczony System musi obejmować wszelkie licencje niezbędne do wdrożenia produkcyjnego oraz uzyskania wsparcia producenta przez okres 2 lat.
- 1.3. System musi zapewniać przetwarzanie danych do niego wysyłanych na terenie EOG (Europejskiego Obszaru Gospodarczego).
- 1.4. System powinien umożliwiać dostęp do dedykowanego dla Zamawiającego zasobu pozwalającego na uruchomieniu minimum 4 maszyn wirtualnych.
- 1.5. Wspierane systemy operacyjne maszyn wirtualnych: Windows 10, macOS, Android, iOS.
- 1.6. System musi zapewniać mechanizm automatycznego sprawdzania nowych wersji oraz automatycznej aktualizacji.
- 1.7. System powinien zapewniać monitoring stanu maszyn wirtualnych.
- 1.8. Obsługa Systemu powinno być możliwa w pełnym zakresie za pomocą graficznego interfejsu użytkownika (Web GUI) oraz wiersza poleceń (CLI).
- 1.9. Komunikacja z panelem zarządzania powinna wykorzystywać szyfrowane połączenie – https.
- 1.10. System powinien zapewniać wsparcie dla wielu kont administratorów, minimum dwóch.
- 1.11. System powinien zapewniać rozliczalność działań administratorów.
- 1.12. System powinien pozwalać na konfigurację kont o różnym poziomie dostępu.
- 1.13. Moduł analizy zagrożeń powinien wykorzystywać m.in. mechanizmy analizy behawiorystycznej opartej o algorytmy sztucznej inteligencji (AI).
- 1.14. System powinien mieć wbudowany mechanizm automatycznej aktualizacji baz zagrożeń.
- 1.15. System powinien automatycznie pobierać do analizy pliki z systemu FortiMail oraz FortiWAF.
- 1.16. System powinien umożliwiać przesyłanie informacji zwrotnej o analizowanym pliku do urzędnika FortiMail umożliwiającej zatrzymanie zainfekowanej przesyłki w kwarantannie oraz do urzędnika FortiGate informacji umożliwiającej aktualizację polityk bezpieczeństwa.
- 1.17. Logowanie zdarzeń powinno być wykonane lokalnie oraz do systemów zewnętrznych.
- 1.18. Powinna być zapewniona integracja z systemami klasy SIEM.
- 1.19. System w zakresie logowania powinien umożliwiać komunikację szyfrowaną.
- 1.20. Wymagane obsługiwane formaty skanowanych plików:
 - 1.20.1. Archiwa: tar, gz, bz2, cab, rar, zip, arj, 7z, ace, tgz
 - 1.20.2. Pliki wykonywalne: exe, msi, bat, dll
 - 1.20.3. Pliki: PDF, MS Office, htm/html, Ink
 - 1.20.4. Adobe Flash

1.20.5. Java Archive: jar

1.20.6. Skrypty: js, vbs, cmd

- 1.21. System powinien posiadać mechanizm tworzenia białych i czarnych list sum kontrolnych plików.
- 1.22. System powinien posiadać mechanizm skanowania adresów URL zawartych w dokumentach.
- 1.23. Monitorowanie zdarzeń w Systemie powinno odbywać się w czasie rzeczywistym, np. statystyki wyników skanowania i być przedstawiane w formie widgetów.
- 1.24. Szczegółowa informacja o zdarzeniu powinna zawierać nazwę zagrożenia, źródło ataku i cel oraz czas wykrycia.
- 1.25. Raporty generowane z poziomu Systemu powinny dotyczyć analizy złośliwego pliku i zawierać charakterystykę ataku – np. modyfikowane pliki w systemie operacyjnym, modyfikacje rejestru, operacje związane z procesami, wywoływane adresy URL, połączenia do serwerów C&C.
- 1.26. System powinien umożliwiać informowanie przy pomocy e-maila o wykryciu zagrożenia.
- 1.27. System powinien umożliwiać przesyłanie plików do analizy poprzez administratora (on-demand).

2. Wdrożenie Systemu obejmuje:

- 2.1. Analizę aktualnych systemów poczty MZ i przygotowanie projektu technicznego rozwiązania zawierającego plan i harmonogram wdrożenia oraz proponowane scenariusze testów funkcjonalnych oraz akceptacyjnych.
- 2.2. Uruchomienie Systemu w środowisku Zamawiającego.
- 2.3. Przygotowanie konfiguracji Systemu i polityk bezpieczeństwa.
- 2.4. Integrację wdrażanego Systemu z systemem FortiAnalyzer, FortiMail, FortiWAF oraz systemem SIEM.
- 2.5. Przeprowadzenie testów funkcjonalnych i akceptacyjnych zainstalowanego Systemu zgodnie z zaakceptowanymi scenariuszami.
- 2.6. Przygotowanie powdrożeniowej dokumentacji technicznej oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis testów obciążeniowych i akceptacyjnych i rozwiązania, opis konfiguracji Systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz Word.
- 2.7. Za pełne wdrożenie Systemu uznaje się wykonanie wszystkich czynności opisanych w pkt. 2.1 do 2.6.

3. Gwarancja dla Systemu

3.1. Definicje:

Awaria - uszkodzenie jednego lub więcej elementów Systemu, ograniczające wydajność lub funkcjonalność lub uniemożliwiające korzystanie z Systemu zgodnie z jego specyfikacją techniczną

Błąd - każde zdarzenie, które nie jest częścią standardowego działania Systemu

Zgłoszenie - poinformowanie Wykonawcy przez przedstawiciela Zamawiającego za pomocą telefonu, wiadomości e-mail, strony internetowej lub system do zgłoszeń udostępnionego przez Wykonawcę na potrzeby realizacji Umowy o zaistniałym wydarzeniu powodującym konieczność podjęcia przez niego interwencji serwisowej. Zgłoszenie może być o zwykłym albo krytycznym priorytecie

Zgłoszenie o krytycznym priorytecie - oznacza wystąpienie Awarii w Systemie, który

uniemożliwia wykorzystywanie podstawowych funkcji Oprogramowania w szczególności uniemożliwiających logowanie do Systemu, przeprowadzania skanowania bezpieczeństwa, pobierania aktualizacji i sygnatur

Zgłoszenie o zwykłym priorytecie - oznacza wystąpienie wszystkich innych Błędów niż wskazane w zgłoszeniu o krytycznym priorytecie

3.2. System musi być objęty gwarancją Wykonawcy przez okres co najmniej 24 miesiące, od daty podpisania protokołu odbioru, która obejmuje:

3.2.1. Zapewnienie wsparcia producenta Systemu.

3.2.2. Zapewnienie polskojęzycznego wsparcia telefonicznego i mailowego w zakresie obsługi i konfiguracji Systemu oraz rozwiązywania problemów związanych z funkcjonalnościami Systemu.

3.2.3. Dostęp do nowych wersji oprogramowania Systemu.

3.2.4. Dostęp do aktualizacji baz zagrożeń.

3.2.5. Dostęp do bazy wiedzy i dokumentacji Systemu.

3.2.6. Zapewnienie informacji o zidentyfikowanych przez producenta Systemu podatnościach w terminie do 3 dni roboczych od momentu publikacji takiej informacji przez producenta.

3.2.7. Umożliwienie zgłaszania problemów za pomocą telefonu, wiadomości e-mail, strony internetowej lub system do zgłoszeń udostępnionego przez Wykonawcę w trybie 24/7/365.

3.2.8. Wsparcie z zakresu obsługi zgłoszeń serwisowych, a w szczególności:

3.2.8.1. Zgłoszenie o zwykłym priorytecie w zakresie Błędów związanych z Systemem z czasem reakcji maksymalnie 72 godziny od chwili wysłania zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 5 Dni Roboczych od dnia przyjęcia zgłoszenia (przez Dni Robocze rozumie się dni od poniedziałku do piątku w godzinach 9:00-17:00, z wyjątkiem dni ustawowo wolnych od pracy i dni wolnych od pracy u Zamawiającego).

3.2.8.2. Zgłoszenie o krytycznym priorytecie - obejmujące pomoc przy wykryciu na serwerach produkcyjnych Awarii, błędów konfiguracji Systemu, z czasem reakcji maksymalnie 2 godziny Dnia Roboczego od chwili wysłania zgłoszenia oraz czasem na przedstawienie propozycji rozwiązania do 3 Dni Roboczych od momentu przyjęcia zgłoszenia.

3.2.8.3. Rozwiązanie problemów będzie realizowane w formie rozmowy telefonicznej lub za pomocą środków online (e-mail, telekonferencja). W przypadku konieczności rozwiązania zgłoszenia w siedzibie Zamawiającego, Wykonawca zobowiązany jest zrealizować zgłoszenie w fizycznej lokalizacji Zamawiającego.

3.2.8.4. Rozwiązanie problemu o priorytecie zwykłym przez Wykonawcę nastąpi w terminie nie przekraczającym 20 Dni Roboczych od potwierdzenia przyjęcia Zgłoszenia.

3.2.8.5. Rozwiązanie problemu o priorytecie krytycznym przez Wykonawcę nastąpi w terminie nie przekraczającym 5 Dni Roboczych od potwierdzenia przyjęcia Zgłoszenia.

4. Przeprowadzenie instruktażu stanowiskowego.

4.1. Zakres instruktażu powinien obejmować przynajmniej:

4.1.1. Omówienie funkcji wdrażanego Systemu.

4.1.2. Działanie mechanizmu wysyłania, pobieranie i skanowania plików.

4.1.3. Konfiguracja mechanizmów skanowania oraz maszyn wirtualnych.

4.1.4. Integracja Systemu z systemami FortiMail, FortiWAF, FortiGate oraz FortiAnalyzer.

4.1.5. Integracja z systemem klasy SIEM.

4.1.6. Zarządzanie logami Systemu.

- 4.1.7. Mechanizmy budowania raportów.
 - 4.1.8. Monitorowanie działania Systemu.
 - 4.1.9. Tworzenie kopii zapasowej Systemu i odtwarzanie w razie awarii.
 - 4.2. Czas trwania instruktażu: co najmniej 8 godzin, podzielonych na min. dwa spotkania
 - 4.3. Zajęcia powinny być przeprowadzone w języku polskim.
 - 4.4. Instruktaż powinien się odbyć w formie telekonferencji na platformie udostępnionej przez Zamawiającego w dni robocze w godzinach 9.00 – 16.00
 - 4.5. Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej
5. Termin realizacji

Umowa zostanie zrealizowana w terminie maksimum 30 dni roboczych (w tym terminie Wykonawca dostarczy, wdroży System oraz przeprowadzi instruktaż stanowiskowy, udzieli prawa do korzystania z systemu i gwarancji) , zgodnie ze złożoną ofertą, od momentu podpisania Umowy.

Gwarancja będzie udzielona na okres co najmniej 24 miesięcy, od daty podpisania protokołu odbioru.