WPZ.230.1.2021
2021-16195

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 i warsztatami szkoleniowymi.

1. Wymagania dla Systemu:

1.1. System powinien zostać dostarczony w formie maszyny wirtualnej, dla środowiska on-premise lub usługi typu cloud uruchomionej w środowisku producenta.
1.2. Dostarczony System musi obejmować wszelkie licencje niezbędne do wdrożenia produkcyjnego oraz uzyskania wsparcia producenta.
1.3. Dla środowiska on-premise preferowane licencje wieczyste (perpetual).
1.4. W wypadku rozwiązania typu cloud System musi zapewniać przetwarzanie danych do niego wysyłanych na terenie EOG (Europejskiego Obszaru Gospodarczego).
1.5. W wersji on-premise System musi umożliwić uruchomienie minimum 4 maszyn wirtualnych i umożliwić rozbudowę do 8 maszyn wirtualnych.
1.6. W wersji cloud System powinien umożliwiać dostęp do dedykowanego dla Zamawiającego zasobu pozwalającego na uruchomieniu minimum 10 maszyn wirtualnych
1.7. Wpierane systemy operacyjne maszyn wirtualnych: Windows 10, macOS, Android, iOS.
1.8. System musi zapewniać mechanizm automatycznego sprawdzania nowych wersji maszyn wirtualnych oraz ich automatycznej aktualizacji
1.9. System powinien zapewniać monitoring stanu maszyn wirtualnych.
1.10. Obsługa Systemu powinno być możliwa w pełnym zakresie za pomocą graficznego interfejsu użytkownika (WebGUI) oraz wiersza poleceń (CLI).
1.11. Komunikacja z panelem zarządzania powinna wykorzystywać szyfrowanie połączenie – https.
1.12. System powinien zapewniać wsparcie dla wielu kont administratorów, minimum dwóch.
1.13. System powinien zapewniać rozliczalność działań administratorów.
1.14. System powinien zapewniać integrację z zewn. mechanizmami uwierzytelniania – LDPA, Active Directory. W tym zakresie komunikacja powinna być szyfrowana.
1.15. W wersji on-premise System powinien zapewniać wsparcie dla klastrów typu High-Availibility.
1.16. Moduł analizy zagrożeń powinien wykorzystywać m.in. mechanizmy analizy behawiorystycznej opartej o algorytmy sztucznej inteligencji (AI).
1.17. System powinien mieć wbudowany mechanizm automatycznej aktualizacji baz zagrożeń.
1.18. System powinien automatycznie pobierać do analizy pliki z systemu FortiMail

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

1.19. System powinien umożliwiać przesyłanie informacji zwrotnej o analizowanym pliku do urządzenia FortiMail umożliwiającej zatrzymanie zainfekowanej przesyłki w kwarantannie oraz do urządzeń FortiGate informacji umożliwiającej aktualizację polityk bezpieczeństwa.

1.20. Logowanie zdarzeń powinno być wykonane lokalnie oraz do systemu zewnętrznego FortiAnalyzer. Powinna być zapewniona również integracja z systemami klasy SIEM. System w zakresie logowania powinien umożliwiać komunikację szyfrowaną.

1.21. Wymagane obsługiwane formaty skanowanych plików:

1.21.1. Archiwa: tar, gz, bz2, cab, rar, zip, arj, 7z, ace, tgz

1.21.2. Pliki wykonywalne: exe, msi, bat, dll

1.21.3. Pliki: PDF, MS Office, htm/html, lnk

1.21.4. Adobe Flash

1.21.5. Java Archive: jar

1.21.6. Skrypty: js, vbs, cmd

1.22. System powinien posiadać mechanizm tworzenia białych i czarnych list sum kontrolnych plików.

1.23. System powinien posiadać mechanizm skanowania adresów URL zawartych w dokumentach.

1.24. Monitorowanie zdarzeń w Systemie powinno odbywać się w czasie rzeczywistym, np. statystyki wyników skanowania i być przedstawiane w formie widgetów.

1.25. Szczegółowa informacja o zdarzeniu powinna zawierać nazwę zagrożenia, źródło ataku i cel oraz czas wykrycia.

1.26. 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.

1.27. System powinien umożliwiać informowanie przy pomocy e-maila o wykryciu zagrożenia.

1.28. Opcjonalnie System powinien umożliwiać przesyłanie plików do analizy poprzez administratora (on-demand).

2. Wdrożenie Systemu obejmuje:

2.1. Analizę aktualnych systemów poczty CeZ i przygotowanie projektu technicznego rozwiązania zawierającego plan i harmonogram wdrożenia oraz proponowane scenariusze testów funkcjonalnych oraz akceptacyjnych.

2.2. Instalację Systemu na udostępnionym przez Zamawiającego środowisku dla wersji on-premise, lub uruchomienie Systemu w środowisku cloud producenta.

2.3. Przygotowanie konfiguracji Systemu i polityk bezpieczeństwa.

2.4. Integrację wdrażanego Systemu z systemem FortiAnalyzer 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

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

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. System musi być objęty gwarancją Wykonawcy przez okres co najmniej 12 miesięcy, od daty podpisania protokołu końcowego, która obejmuje:
- 3.1.1. Zapewnienie wsparcia producenta Systemu
- 3.1.2. Zapewnienie polskojęzycznego wsparcia telefonicznego i mailowego w zakresie obsługi i konfiguracji Systemu oraz rozwiązywania problemów związanych z funkcjonalnościami Systemu
- 3.1.3. Dostęp do nowych wersji oprogramowania Systemu
- 3.1.4. Dostęp do aktualizacji baz zagrożeń
- 3.1.5. Dostęp do bazy wiedzy i dokumentacji Systemu
- 3.1.6. Zapewnienie informacji o zidentyfikowanych przez producenta Systemu podatnościach w terminie do 3 dni roboczych od momentu publikacji takiej informacji przez producenta.
- 3.1.7. Umożliwienie zgłaszania problemów za pomocą poczty elektroniczne i poprzez stronę WWW w trybie 24/7/365
- 3.1.8. Wsparcie z zakresie obsługi zgłoszeń serwisowych, a w szczególności:
  - 3.1.8.1. Zgłoszenie o zwykłym priorytecie w zakresie błędów związanych z Oprogramowaniem 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)
  - 3.1.8.2. Zgłoszenie o krytycznym priorytecie - obejmujące pomoc przy wykryciu na serwerach produkcyjnych błędów krytycznych, konfiguracji Oprogramowania 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.
  - 3.1.8.3. 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.

4. Przeprowadzenie warsztatów szkoleniowych

4.1. Zakres warsztatów 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, 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

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

4.1.9. Tworzenie kopii zapasowej Systemu i odtwarzanie w razie awarii

4.2. Czas trwania warsztatów: co najmniej 8 godzin, podzielonych na min. dwa spotkania

4.3. Zajęcia powinny być przeprowadzone w języku polskim

4.4. Warsztaty powinny 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 20 dni roboczych, zgodnie ze złożoną ofertą, od momentu podpisania Umowy.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706