Załącznik nr 1

SZCZEGÓŁOWY OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiot zamówienia: Dostawa systemu typu sandbox wraz z wdrożeniem.

Zamówienie obejmuje:

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, wsparciem technicznym producenta i warsztatami powdrożeniowymi.

1. Wymagania szczegółowe dotyczące funkcjonalności systemu

Wymagania dla systemu:

1. System powinien zostać dostarczony w formie maszyny wirtualnej, dla środowiska on-premise, zgodnej ze środowiskiem wirtualizacyjnym zamawiającego - VMware vSphere;
2. Zamawiający wyklucza dostarczenie systemu sandbox w formie usługi chmurowej i formie osobnego urządzenia;
3. Dostarczony System musi obejmować wszelkie licencje niezbędne do wdrożenia produkcyjnego oraz uzyskania wsparcia producenta;
4. System musi pozwalać technicznie i licencyjnie na uruchomienie minimum 8 maszyn wirtualnych i zainstalowanie na nich systemu operacyjnego przez Zamawiającego na zasadzie BYOL;
5. System musi zapewniać monitorowanie stanu wirtualnych maszyn;
6. System musi automatycznie pobierać do analizy pliki z systemu FortiMail wykorzystywanego przez Zamawiającego;
7. System musi zapewniać wsparcie dla klastrów typu High-Availibility;
8. Moduł analizy zagrożeń musi wykorzystywać m.in. mechanizmy analizy behawiorystycznej opartej o algorytmy sztucznej inteligencji (AI);
9. System musi mieć wbudowany mechanizm automatycznej aktualizacji baz zagrożeń z zasobów producenta;
10. System musi posiadać mechanizm tworzenia białych i czarnych list sum kontrolnych plików;
11. System musi posiadać mechanizm skanowania adresów URL zawartych w dokumentach;

Wymagania dla zarządzania systemem:

1. System musi mieć możliwość zarządzania/obsługi poprzez:
   - graficzny interfejs (GUI). Interfejs graficzny musi być dostępny przez przeglądarkę internetową protokołem HTTP i HTTPS (obsługiwać SSL).
   - przez linię poleceń (CLI). Interfejs CLI musi mieć możliwość zarządzania przez połączenie SSH jak i przez wbudowany w system, dostępny również z GUI, własny interfejs CLI.

2. System musi wspierać obsługę logowania/uwierzytelniania użytkownika kontami:
   - tworzonymi lokalnymi
   - kontami opartymi o LDAP, LDAPS i RADIUS.

3. System musi posiadać funkcję tworzenia kont administratora i użytkownika oraz grup użytkowników wraz z granulacją nadawania uprawnień do składowych elementów systemu. Musi posiadać możliwość tworzenia wielu kont administratora i użytkownika.

Funkcjonalności, które muszą współpracować z systemem FortiMail, FortiGate oraz FortiAnalyzer posiadanymi przez Zamawiającego:

1. System musi automatycznie pobierać do analizy pliki z systemu FortiMail;
2. System musi umożliwiać przesyłanie informacji zwrotnej o analizowanym pliku do systemu FortiMail umożliwiając zatrzymanie zainfekowanej przesyłki w kwarantannie oraz do urządzeń FortiGate informacji umożliwiającej aktualizację polityk bezpieczeństwa;
3. Logowanie zdarzeń musi być wykonane lokalnie oraz do systemu zewnętrznego – FortiAnalyzer;
4. System musi być gotowy do wdrożenia i integracji z innymi elementami i urządzeniami, odpowiadającymi za bezpieczeństwo infrastruktury, posiadanymi przez zamawiającego, takimi jak FortiGate, FortiAnalyzer, FortiClient, FortiMail, FortiWeb oraz działać w oparciu o dane wymieniane między tymi systemami, za pomocą ich wbudowanej funkcjonalności – Security Fabric;

Wymagane funkcje działania systemu sandbox wspierające bezpieczeństwo:

1. System musi zapewniać obsługę skanowania(co najmniej):
   - Archiwa: tar, gz, bz2, cab, rar, zip, arj, 7z, ace, tgz;
   - Pliki wykonywalne: exe, msi, bat, dll;
   - Pliki: PDF, MS Office, htm/html, lnk;
   - Adobe Flash;
   - Java Archive: jar;
   - Skrypty: js, vbs, cmd, powershell;
   - adresów URL zawartych w dokumentach.

2. System musi zawierać obsługę skanowania danych/plików przesyłanych z wykorzystaniem następujących protokołów:

- w przypadku integracji z FortiGate - http, ftp, smtp, pop3, imap oraz ich odpowiedników wykorzystujących protokół SSL;
- w przypadku integracji z FortiMail – smtp, imap, pop3;
- w przypadku integracji z FortiClient – http, ftp, smb.

3. Monitorowanie zdarzeń w Systemie powinno odbywać się w czasie rzeczywistym, np. statystyki wyników skanowania powinny być przedstawiane w formie widgetów;

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

5. System musi umożliwiać informowanie przy pomocy e-maila o wykryciu zagrożenia;

6. Raporty generowane z poziomu Systemu muszą 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.

2. Wymagania dodatkowe:

Wykonawca zobowiązany jest do dostarczenia:

a. 8 licencji MS ESD Windows Professional 11 64-bit All Languages;
b. 8 licencji MS ESD Office Professional 2021 Win All Languages.

3. Wdrożenie systemu musi objąć co najmniej:

1. Instalację Systemu na udostępnionym przez Zamawiającego środowisku dla wersji on-premise;
2. Uruchomienie w systemie sandbox 8 maszyn wirtualnych i zainstalowanie na nich systemu operacyjnego oraz pakietu Office dostarczonego przez Wykonawcę;
3. Przygotowanie konfiguracji Systemu i polityk bezpieczeństwa;
4. Integrację wdrażanego Systemu z systemem FortiAnalyzer, FortiMail oraz FortiGate;
5. Przygotowanie powdrożeniowej dokumentacji technicznej oraz dokumentacji użytkownika Systemu zawierającej architekturę rozwiązania, spis wszystkich wdrożonych polityk bezpieczeństwa, opis konfiguracji Systemu (w tym nietypowe ustawienia) oraz instrukcję dla użytkownika/administratora Systemu w języku polskim, w formie elektronicznej – PDF oraz Word.

4. Gwarancja systemu:

System musi być objęty gwarancją producenta przez okres **co najmniej 12 miesięcy**, od daty podpisania protokołu końcowego, która obejmuje co najmniej dostęp do nowych wersji oprogramowania Systemu oraz dostęp do aktualizacji baz zagrożeń.

5. Warsztaty powdrożeniowe:

Zakres warsztatów powinien obejmować co najmniej:

a. Omówienie funkcji wdrażanego Systemu;
b. Omówienie działania mechanizmu wysyłania, pobierania i skanowania plików;
c. Omówienie konfiguracji mechanizmów skanowania oraz maszyn wirtualnych;
d. Omówienie integracji Systemu z systemami FortiMail, FortiGate oraz FortiAnalyzer;
e. Omówienie mechanizmu budowania raportów;
f. Omówienie monitorowania działania Systemu;
g. Omówienie tworzenia kopii zapasowej Systemu i odtwarzania w razie awarii

- Czas trwania warsztatów: co najmniej 16 godzin, podzielonych na min. 4 spotkania;
- Zajęcia muszą być przeprowadzone w języku polskim;
- Warsztaty musza się odbyć w formie wideokonferencji w dni robocze w godzinach 9.00 – 14.00;
- Uczestnikom zapewnione zostaną materiały dydaktyczne w formie elektronicznej w języku polskim;