NARODOWY INSTYTUT ZDROWIA PUBLICZNEGO
PAŃSTWOWY INSTYTUT BADAWCZY

Załącznik nr 1 do Zapytania ofertowego

OPIS PRZEDMIOTU ZAMÓWIENIA

Subskrypcja na 12 miesięcy, na oprogramowanie do urządzeń zabezpieczających Fortinet posiadanych przez Zamawiającego wraz z zakupem nowej subskrypcji FortiAnalyzer na 12 miesięcy.

1. FortiGate 500E – 2 szt. (urządzenia pracujące w konfiguracji HA) (data wygaśnięcia 2024-07-23)

   Subskrypcja zawierająca: FG-500E 24x7 Unified Threat Protection 1Y, Unified Threat Protection (UTP) (IPS, Advanced Malware Protection, Application Control, Web & Video Filtering, Antispam Service, and 24x7 FortiCare)

2. FortiWeb-400D – 1 szt. (data wygaśnięcia 2024-07-23)

   Subskrypcja zawierająca: Standard Bundle (24x7 FortiCare plus AV, FortiWeb Security Service, and IP Reputation), Secure RMA Service (pozostawienie dysku u Zamawiającego w przypadku jego wymiany lub wymiany urządzenia)

3. FortiMail-VM01 – 1 szt. (data wygaśnięcia 2024-06-01)

   Subskrypcja zawierająca: FortiMail-VM01 – 24x7 FortiCare and FortiGuard Base Bundle Contract, FortiMail Cloud Sandbox - Cloud Sandbox for FortiMail

4. FortiAnalyzer-VM - subskrypcja:

Wymagania ogólne

W ramach postępowania wymaganym jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń.
Rozwiązanie musi zostać dostarczone w postaci komercyjnej platformy działającej w środowisku wirtualnym lub w postaci komercyjnej platformy działającej na bazie linux w środowisku wirtualnym, z możliwością uruchomienia na co najmniej następujących hypervisorach: VMware ESX/ESXi wersje: 5.0, 5.1, 5.5, 6.0, 6.5, 6.7; Microsoft Hyper-V wersje: 2008 R2, 2012, 2012 R2, 2016; Citrix XenServer 6.0+, Open Source Xen 4.1+, KVM, Amazon Web Services (AWS), Microsoft Azure, Google Cloud (GCP).

Interfejsy, dysk:

1. System musi obsługiwać co najmniej 4 interfejsy sieciowe oraz wspierać powierzchnię dyskową o pojemności 10 TB.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 20 GB logów na dzień.
2. Rozwiązanie musi umożliwiać kolekcjonowanie logów z co najmniej 1000 systemów.

W ramach centralnego systemu logowania, raportowania i korelacji muszą być realizowane co najmniej poniższe funkcje:

Logowanie

1. Podgląd logowanych zdarzeń w czasie rzeczywistym.
2. Możliwość przeglądania logów historycznych z funkcją filtrowania.
3. System musi oferować predefiniowane (lub mieć możliwość ich konfiguracji) podręczne raporty graficzne lub tekstowe obrazujące stan pracy urządzenia oraz ogólne informacje dotyczące statystyk ruchu sieciowego i zdarzeń bezpieczeństwa. Muszą one obejmować co najmniej:
   a) Listę najczęściej wykrywanych ataków,
   b) Listę najbardziej aktywnych użytkowników,
   c) Listę najczęściej wykorzystywanych aplikacji,
   d) Listę najczęściej odwiedzanych stron www,
   e) Listę krajów , do których nawiązywane są połączenia,
   f) Listę najczęściej wykorzystywanych polityk Firewall,
   g) Informacje o realizowanych połączeniach IPSec,
4. Rozwiązanie musi posiadać możliwość przesyłania kopii logów do innych systemów logowania i przetwarzania danych. Musi w tym zakresie zapewniać mechanizmy filtrowania dla wysyłanych logów.
5. Komunikacja systemów bezpieczeństwa (z których przesyłane są logi) z oferowanym systemem centralnego logowania musi być możliwa co najmniej z wykorzystaniem UDP/514 oraz TCP/514.
6. System musi realizować cykliczny eksport logów do zewnętrznego systemu w celu ich długo czasowego składowania. Eksport logów musi być możliwy za pomocą protokołu SFTP lub na zewnętrzny zasób sieciowy.

Raportowanie

W zakresie raportowania system musi zapewniać:

1. Generowanie raportów co najmniej w formatach: PDF, CSV.
2. Predefiniowane zestawy raportów, dla których administrator systemu może modyfikować parametry prezentowania wyników.
3. Funkcję definiowania własnych raportów.
4. Możliwość spolszczenia raportów.
5. Generowanie raportów w sposób cykliczny lub na żądanie, z możliwością automatycznego przesłania wyników na określony adres lub adresy email.

Korelacja logów

W zakresie korelacji zdarzeń system musi zapewniać:

1. Korelowanie logów z określeniem urządzeń, dla których ten proces ma być realizowany.
2. Konfigurację powiadomień poprzez: e-mail, SNMP w przypadku wystąpienia określonych zdarzeń sieciowych, systemowych oraz bezpieczeństwa.
3. Wybór kategorii zdarzeń, dla których tworzone będą reguły korelacyjne. System korelować zdarzenia co najmniej dla następujących kategorii zdarzeń:
   - Malware,
   - Aplikacje sieciowe,
   - Email,
   - IPS,
   - Traffic,
   - Systemowe: utracone połączenie VPN, utracone połączenie sieciowe.

4. Funkcję analizy logów archiwalnych względem aktualnej wiedzy producenta o zagrożeniach, w celu wykrycia potencjalnych stacji - narażonych na zagrożenie w ostatnim czasie.

Zarządzanie

1. System logowania i raportowania musi mieć możliwość zarządzania lokalnego z wykorzystaniem protokołów: HTTPS oraz SSH lub producent rozwiązania musi dostarczać dedykowanej konsoli zarządzania, która komunikuje się z rozwiązaniem przy wykorzystaniu szyfrowanych protokołów.

   a) Proces uwierzytelniania administratorów musi być realizowany w oparciu o: lokalną bazę, Radius, LDAP, PKI.

2. System musi umożliwiać zdefiniowanie co najmniej 4 administratorów z możliwością określenia praw dostępu do logowanych informacji i raportów z perspektywy poszczególnych systemów, z których przesyłane są logi.

Serwisy, licencje i gwarancja

System musi być objęty serwisem producenta przez okres 12 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

NARODOWY INSTYTUT ZDROWIA PUBLICZNEGO
PAŃSTWOWY INSTYTUT BADAWCZY

Numery seryjne urządzeń Fortinet posiadanych przez Zamawiającego:

FortiMail-VM01:

FEVM010000186755

Fortigate-500E:

FG5H0E5819901716

FG5H0E5818907482

FortiWeb-400D:

FV400DTA19000061

W przypadku zaproponowania przez Wykonawcę rozwiązania równoważnego, Wykonawca będzie zobowiązany do:

- dostarczenia oraz konfiguracji urządzeń zabezpieczających o nie gorszych parametrach niż wyszczególnione powyżej do siedziby Zamawiającego do dnia 01.06.2024 r.

- przeniesienia pełnej konfiguracji z obecnych urządzeń zabezpieczających na nowe urządzenia dostarczone do dnia 01.06.2024 r., z zachowaniem obecnej pełnej integracji urządzeń,

- przeszkolenia czterech Pracowników Działu Informatycznego w siedzibie u Zamawiającego z obsługi nowych urządzeń do 01.06.2024 r.,

Za wszelkie przestoje i niedogodności związane z wymianą urządzeń i przeniesieniem konfiguracji Wykonawca ponosi odpowiedzialność finansową.