

Zadanie nr 2

Wymagania dla Oferentów w zakresie zamawianego Fortinet FortiAnalyzer (licencje na serwer logów i raportów firewalla) według wariantów

Przedmiotem zamówienia jest zakup wraz z dostawą Fortinet FortiAnalyzer (licencje na serwer logów i raportów firewalla) dla dwóch lokalizacji wraz ze wsparciem serwisowym

Wariant I – na 1 rok;

Wariant II – na 3 lata;

czyli:

- 1) FAZ-VM-GB5 - licencja na produkt Fortinet FortiAnalyzer-VM (maszyna wirtualna z możliwością logowania 5 GB/dzień i 3 TB pojemności);
- 2) FC1-10-LV0VM-248-02-12/36: Produkt Fortinet wsparcie serwisowe FortiCare dla FortiAnalyzer VM

Wymagania Ogólne

W ramach postępowania wymagane jest dostarczenie centralnego systemu logowania, raportowania i korelacji, umożliwiającego centralizację procesu logowania zdarzeń sieciowych, systemowych oraz bezpieczeństwa w ramach całej infrastruktury zabezpieczeń w placówce SP ZOZ MSWiA W Koszalinie, w lokalizacji Koszalin i Słupsk.

Niezbędne cechy: integracja z Fortinet Security Fabric

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:

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 **5 GB** logów na dzień.

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 protokołów 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.

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.

Serwis i licencje

1. Wsparcie: System musi być objęty serwisem producenta przez okres 12 lub 36 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7 w zależności od wariantu, który zostanie wybrany przez Zamawiającego.