Szczegółowy opis przedmiotu zamówienia
„Zakup urządzeń wirtualnych”

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 werje:, 7.x, 8,x; Microsoft Hyper-V wersje:, 2022 2025KVM,

Interfejsy, Dysk:

System musi obsługiwać co najmniej 4 interfejsy sieciowe.

Parametry wydajnościowe:

1. System musi być w stanie przyjmować minimum 5 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

1. System musi być objęty serwisem producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.
2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

System uwierzytelniania, autoryzacji i kontroli dostępu

Oferowane rozwiązanie musi pozwalać na centralne zarządzenie kontami użytkowników oraz procesem uwierzytelnienia – w tym celu musi zapewniać wszystkie wymienione poniżej funkcje.

Dopuszcza się aby poszczególne elementy wchodzące w skład systemu były zrealizowane w postaci osobnych, komercyjnych platform wirtualnych lub komercyjnych aplikacji instalowanych na platformach ogólnego przeznaczenia. W przypadku implementacji programowej dostawca musi zapewnić niezbędne, odpowiednio zabezpieczone systemy operacyjne dla poszczególnych komponentów.

Parametry systemu

Poszczególne elementy wchodzące w skład systemu muszą zapewniać obsługę:

- 4 wirtualnych interfejsów sieciowych.
- Możliwość uruchomienia w środowiskach: Microsoft Hyper-V Server, 2022, 2025; VMware ESXi, ESX wersje:, 7.x,8.x; KVM,.

Parametry wydajnościowe i licencyjne

System musi obsługiwać co najmniej:

- Uwierzytelnianie dla 100 użytkowników.
- 200 tokenów dla uwierzytelniania dwuskładnikowego
- 30 klientów protokołu RADIUS (urządzeń NAS, które można podpiąć do systemu).
- Możliwość zdefiniowania co najmniej 10 grup użytkowników,
- 5 lokalnych centrów certyfikacji (CA).
- Możliwość wygenerowania 100 certyfikatów dla użytkowników.

Wymagania ogólne

System musi zapewniać nie mniej niż:

1. Możliwość pracy w konfiguracji HA (High Availability) z trybem Active-Passive lub Active-Active w celu zwiększenia niezawodności.
2. Graficzną reprezentację statusu uwierzytelnionych użytkowników.
3. Logowanie wszystkich zdarzeń uwierzytelniania wraz z ich statusem, szczegółami dotyczącymi powodów niepowodzenia oraz nazwą użytkownika:

a. Lokalnie.

b. Zdalnie w oparciu o protokół Syslog.

4. Konfigurację Captive Portalu.

Wymagania funkcjonalne – uwierzytelnianie

Celem realizacji funkcji uwierzytelniających, system musi zapewniać nie mniej niż:

1. Lokalną, wbudowaną bazę użytkowników.
2. Przechowywanie następujących informacji o użytkowniku: nazwa, imię i nazwisko, adres email, numer telefonu, adres, kraj, województwo.
3. Możliwość zdefiniowania co najmniej 3 indywidualnie konfigurowalnych pól dla każdego z użytkowników.
4. Możliwość importu informacji o użytkownikach z zewnętrznego serwera LDAP lub pliku CSV.
5. Konfigurowalną politykę haseł użytkowników w ramach której możliwym jest określenie:

a. poziomu złożoności hasła (jego długości minimalnej, występowania małych i dużych liter, cyfr i znaków specjalnych),

b. czasu ważności hasła,

6. Konfigurowalną politykę blokowania kont, która będzie uwzględniać:

a. ilość nieudanych logowań,

b. czas blokowania konta,

c. okres nieaktywności, po którym konto jest blokowane.

7. Możliwość odzyskiwania haseł:

a. z wykorzystaniem adresu email,

b. z wykorzystaniem pytania pomocniczego.

8. Obsługę protokołu RADIUS zgodną z RFC, w tym zakresie system musi oferować:

a. wbudowany serwer RADIUS,

b. integrację z zewnętrznymi serwerami RADIUS – praca jako klient.

9. Obsługę protokołu LDAP, w tym zakresie system musi oferować:

a. wbudowany serwer LDAP,

b. możliwość zautomatyzowanej synchronizacji z zewnętrznym serwerem LDAP (zarówno kont użytkowników jak i atrybutów LDAP).

10. Obsługę protokołu SAML - Identity Provider (IdP) proxy.
11. Realizację funkcji SSO (Single Sign On) w oparciu o:

a. integrację z Active Directory, również bez konieczności instalacji dodatkowego oprogramowania na kontrolerach domeny,

b. dedykowaną aplikację instalowaną na stacjach roboczych z systemem Windows,

c. kontekst użytkownika przesyłany z serwera RADIUS,

d. informacje uzyskiwane poprzez protokół Syslog,

Wymagania funkcjonalne – uwierzytelnianie dwuskładnikowe

Realizując uwierzytelnianie dwuskładnikowe, system musi zapewniać nie mniej niż:

1. Obsługę dla tokenów sprzętowych (hardware).
2. Wsparcie dla tokenów programowych (software token) dla takich systemów operacyjnych jak iOS, Android, Windows Phone (8 i 8.1) oraz Windows 10 Mobile.

Wymagania funkcjonalne – 802.1x

System powinien umożliwiać realizację uwierzytelniania z wykorzystaniem protokołu 802.1x, spełniając nie mniej niż następujące warunki:

1. Obsługa co najmniej poniższych protokołów EAP:

a. PEAP,

b. EAP-TTLS,

c. EAP-TLS,

d. EAP-GTC.

2. Wsparcie dla uwierzytelnienia w oparciu o adres MAC (MAC based authentication).
3. Zarządzanie certyfikatami (w oparciu o własne CA) celem wykorzystania w ramach PEAP, TTLS, TLS.

Wymagania funkcjonalne – zarządzanie certyfikatami

System powinien spełniać następujące wymagania w zakresie zarządzania certyfikatami, nie mniej niż:

1. Obsługa wbudowanego CA (Certificate Authority).
2. Obsługa CA pośredniczących (Intermediate CA).
3. Ręczne generowanie certyfikatów z wykorzystaniem interfejsu graficznego.
4. Możliwość pobrania wygenerowanych certyfikatów.
5. Możliwość podpisywania certyfikatów z wykorzystaniem protokołu SCEP.
6. Możliwość automatycznego i ręcznego generowania certyfikatów z wykorzystaniem protokołu SCEP.
7. Możliwość generowania certyfikatów typu wildcard.
8. Realizacja CRL (Certificate Revocation List).
9. Wsparcie dynamicznego odwoływania certyfikatów z wykorzystaniem protokołu OCSP (RFC2560).
10. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Zarządzanie

1. Zarządzanie w oparciu o protokół HTTPS (interfejs graficzny) z wykorzystaniem przeglądarki.

2. System udostępnia graficzny interfejs zarządzania poprzez szyfrowane połączenie HTTPS.
3. Tworzenie kopii bezpieczeństwa konfiguracji z poziomu graficznego interfejsu zarządzającego (GUI) oraz na zewnętrzny serwer FTP/SFTP w oparciu o harmonogram, który będzie umożliwiał wskazanie konkretnego czasu kiedy proces ma się rozpocząć.
4. Powinna istnieć możliwość zdefiniowania co najmniej 4 lokalnych kont administracyjnych.

Serwis i usługi

1. Wymaga się aby dostawa obejmowała również serwis producenta przez okres 24 miesięcy, upoważniającym do aktualizacji oprogramowania oraz wsparcia technicznego w trybie 24x7.

2. Wykonawca musi zapewnić pierwszą linię wsparcia w języku polskim trybie 8x5. W celu realizacji wymogu wymagane jest posiadanie co najmniej dwóch inżynierów z aktualnym certyfikatem producenta oferowanego rozwiązania (jeżeli producent oferowanego rozwiązania stosuje stopniowy system certyfikacji to co najmniej jeden inżynier musi posiadać najwyższy stopień certyfikacji dla danego rozwiązania) oraz ISO 9001 , ISO 27001 i ISO 22301 w zakresie serwisowania urządzeń informatycznych. Wszystkie certyfikaty należy dołączyć do oferty.

3. Zamawiający wymaga dostarczenia 100 tokenów mobilnych do dwu-składnikowego uwierzytelniania, z licencją wieczystą od producenta oferowanego systemu uwierzytelniania, autoryzacji i kontroli dostępu. Tokeny muszą zapewniać wsparcie dla systemów dla iOS oraz Android.