ZP.CI.262.13.2025

Załącznik nr 1

Opis przedmiotu zamówienia - oprogramowanie do Laboratorium Cyberbezpieczeństwa

1. **Przedmiot zamówienia**
   Zakup, dostawa i wdrożenie systemu do Laboratorium Cyberbezpieczeństwa (LABCYBER) wraz ze wsparciem powdrożeniowym na okres 24 miesięcy.
2. **W ramach dostawy oprogramowania Wykonawca zapewni**
   2.1. Dostarczenia 2 letnich licencji na oprogramowanie wchodzące w skład systemu LABCYBER w liczbie umożliwiającej funkcjonowanie laboratorium (15 użytkowników).
   2.2. Wykonanie prac wdrożeniowych na infrastrukturze Zamawiającego (przygotowanie planu przedwdrożeniowego, instalacja systemu w wyznaczonych miejscach przez Zamawiającego, wdrożenie na podstawie przygotowanego planu przedwdrożeniowego, konfiguracja oprogramowania, testy i uruchomienie produkcyjne.
   2.3. Konfiguracja systemu powinna zapewnić prowadzenie zajęć w celu zaprezentowania możliwości systemu w celach edukacyjnych.
   2.4. Instruktaż stanowiskowy dla 2 administratorów z w zakresie administracji, obsługi oraz utrzymania dostarczonego systemu.
   2.5. Przygotowanie dokumentacji powdrożeniowej, w tym Instrukcji obsługi systemu dla studentów, w języku polskim (wersja elektroniczna w formacie PDF).
   2.6. Wgranie niezbędnych licencji i przeniesienie ich na Politechnikę Warszawską.
   2.7. Wykonanie wszystkich prac wdrożeniowych w ciągu 30 dni od daty podpisania umowy.
3. **Wymagania podstawowe**
   3.1. W skład systemu LABCYBER powinny wchodzić komponenty obejmujące funkcjonalności: EDR, UTM, IDPS.
   3.2. System powinien umożliwiać założenie kont 15 użytkowników typu „super-user” do zdalnego zarządzania EDR.
   3.3. System musi umożliwiać jego instalację na systemie operacyjnym Microsoft Windows Server Standard 2022.
   3.4. Interfejs oprogramowania oraz konfiguracji musi być w całości dostępny z poziomu przeglądarki internetowej (Microsoft Edge, wersja 130 lub nowsza, Mozilla Firefox, wersja 132 lub nowsza, Google Chrome, wersja 131 lub nowsza).
   3.5. Dopuszczalnym językiem interfejsu jest język polski i angielski.
4. **Wymagania funkcjonalne EDR**
   4.1. Wykrywanie zagrożeń
      4.1.1. Sortowanie informacji według popularności, reputacji, podpisów cyfrowych, zachowania i informacji kontekstowych.
      4.1.2. Automatyzacja procesu wykrywania zagrożeń i dostosowanie go do charakterystyki środowiska danej firmy.
      4.1.3. Łatwe wykrywanie zagrożeń, w tym również APT i ataków ukierunkowanych.
      4.1.4. Przeglądanie kompletnych danych nt. infekcji i ataków w sieci firmowej, w tym o czasie ich wykonania, użytkownikach, którzy je uruchomili, długości ich trwania oraz urządzeniach nimi dotkniętych.

4.1.5. Przeglądanie i blokowanie ataków i infekcji powinny bazować na wskaźnikach obejmujących co najmniej: hashe, zmiany rejestru, modyfikacje plików i połączeniach sieciowych.
4.1.6. Dane o wykrytych zagrożeniach powinny być przechowywane lokalnie.
4.2. Wykrywanie anomalii i zachowań niebezpiecznych
4.2.1. Kontrola aktywności plików wykonywalnych i szybka ocena, czy wykonywany proces jest bezpieczny, albo podejrzany.
4.2.2. Szybka weryfikacja, czy dana aktywność była typowa, czy też nie powinna zostać zainicjowana przez konkretnego użytkownika.
4.3. Wykrywanie zdarzeń (analiza źródła problemu)
4.3.1. Łatwe przeglądanie wszystkich zarejestrowanych alarmów.
4.3.2. Łatwa analiza źródła problemu.
4.4. Naruszenia polityki bezpieczeństwa
4.4.1. Otwarta architektura powinna zapewniać elastyczność konfiguracji systemu.
4.4.2. Wykrywania naruszeń polityk użycia pewnych rodzajów oprogramowania, np. torrenty, dyski chmurowe, przeglądarki Tor oraz serwery uruchamiane przez użytkowników lub inne niepożądane programy.
4.5. Zapobieganie i reakcja
4.5.1. Wbudowany zestaw reguł powinien umożliwiać tworzenie własnych zasad reakcji na wykryte zdarzenia.
4.5.2. Blokowanie plików za pomocą hasha lub przerwanie i poddanie kwarantannie poszczególnych procesów.
4.5.3. Możliwość odizolowania urządzenia od sieci firmowej lub jego zdalne wyłączenie.

5. Wymagania funkcjonalne UTM

5.1. Podstawowe funkcje ochronne:
5.1.1. Firewall typu statefull packet filter.
5.1.2. Moduł AV - zintegrowany.
5.1.3. Wbudowany system ochrony przed włamaniami, exploitami (IPS).
5.1.4. Wbudowany moduł antyspamowy.
5.1.5. Filtrowanie złośliwych stron.
5.1.6. Producent bez złośliwych URL.
5.2. Zaawansowane funkcje ochronne:
5.2.1. Możliwość skanowania szyfrowanego ruchu http.
5.2.2. Kontrola aplikacji/firewall aplikacyjny.
5.2.3. Zabezpieczenie przed wyciekiem danych (DLP).
5.2.4. Piaskownica dla wykrywania nieznanych/nierozpoznanych zagrożeń.
5.2.5. Ochrona przez atakami typu DDoS.
5.2.6. Funkcjonować jako reverse proxy.
5.3. VPN
5.3.1. Dedykowane oprogramowanie dla VPN Client-To-Site.
5.3.2. Tworzenie tuneli Site-To-Site.
5.4. Obsługa sieci bezprzewodowych
5.4.1. Wbudowany moduł WiFi.
5.4.2. Zarządzanie centralne AP.
5.4.3. Wbudowane gniazdo na kartę SIM/port USB dla modemu.
5.5. Administrowanie
5.5.1. Raportowanie - tworzenie zestawień logów w formie tekstowej/graficznej.
5.5.2. Zbieranie i przesyłanie logów systemowych.

5.5.3. Metody uwierzytelnienia – lokalna, AD, LDAP, RADIUS, dwuetapowa.
5.5.4. Zarządzanie poprzez oprogramowanie, stronę WWW, konsolę.
5.5.5. Zainstalowany system operacyjny.
5.5.6. Bezpośredni dostęp do plików OS.
5.5.7. Bez konieczności używania wiersza poleceń do konfiguracji urządzenia.

5.6. Routing, obsługa ruchu w sieci
5.6.1. Zarządzanie ruchem w sieci wg aplikacji.
5.6.2. Zarządzanie pasmem wg aplikacji.
5.6.3. Kolejkowanie ruchu/ priorytetyzacja ruchu/ zarządzanie pasmem.
5.6.4. Możliwość automatycznego przełączenia na zapasowego dostawcę internetu.
5.6.5. Równoważenie pasma internetu.

6. Wsparcie powdrożeniowe

6.1. Wykonawca zapewni usługę wsparcia powdrożeniowego dla systemu.

6.2. Usługa wsparcia powdrożeniowego musi uprawniać Zamawiającego przez okres 24 miesięcy liczonych od dnia podpisania Protokołu Odbioru bez zastrzeżeń do:

a) Telefonicznego i mailowego wsparcia w języku polskim przez 5 dni w tygodniu (od poniedziałku do piątku z wykluczeniem dni ustawowo wolnych od pracy), od godziny 8:00 do 18:00.
b) W przypadku zgłoszeń wad o wysokim priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 1 godzina, czas rozwiązania problemu maksymalnie w 2 dni robocze liczone od dnia zgłoszenia.
c) W przypadku zgłoszeń wad o normalnym priorytecie – czas reakcji na zgłoszenie nie dłuższy niż 4 godziny, czas rozwiązania problemu maksymalnie w 5 dni robocze liczone od dnia zgłoszenia.
d) Dodatkowych konsultacji telefonicznych i mailowych w zakresie działania systemu.
e) Instruktażu telefonicznego i mailowego dotyczącego systemu.
f) Konsultacji telefonicznych i mailowych w zakresie konfiguracji zaoferowanego rozwiązania w celu usprawnienia jego działania.
g) Aktualizacji oprogramowania do najnowszych wersji wykonywanych przez Wykonawcę w siedzibie Zamawiającego lub zdalnie/online.
h) Backupu przy podnoszeniu wersji systemu wykonywany przez Wykonawcę w siedzibie Zamawiającego lub zdalnie/online.
i) Obsługi zgłoszeń w siedzibie Zamawiającego lub zdalnie/online.