*Sfinansowano w ramach reakcji Unii na pandemię COVID-19*

Załącznik nr 1 do SWZ
Opis Przedmiotu Umowy

## CZĘŚĆ I

Zamawiający posiada urządzenie klasy UTM firmy Barracuda.

Przedmiotem zamówienia jest:

1. Przedłużenie wsparcia do tego urządzenia na okres 3 lat
   a) Energize Updates Subscription,
   b) Malware Protection Subscription,
   c) Instant Replacement Subscription,
2. Dostarczenie nowego identycznego modelu urządzenia (w celu uruchomienia funkcjonalności HA) wraz ze wsparciem na okres 3 lat
   a) Energize Updates Subscription,
   d) Malware Protection Subscription,
   e) Instant Replacement Subscription,

   oraz kompatybilnym przewodem DAC do bezpośredniego połączenia obu urządzeń.
3. Udzielenie zdalnego wsparcia technicznego podczas uruchomienia funkcjonalności HA. Wsparcie w formie konsultacji telefonicznych i mailowych lub połączenia zdalnego. Zagwarantowany czas: minimalnie 4 h – maksymalnie 8 h.

Dokładne dane dotyczące modelu urządzenia oraz obecnej umowy serwisowej można uzyskać u Zamawiającego. Powołując się na art. 131 ust. 2 Pzp dane szczegółowe zostaną udostępnione podmiotom uczestniczącym w postępowaniu po odbyciu przez Wykonawcę wizji lokalnej.

## CZĘŚĆ II

System klasy SIEM (Security Information & Event Management)

| **1** | **Charakterystyka (wymagania minimalne)** |
|---|---|
| 1.1 | Proponowane rozwiązanie w zakresie monitorowania musi być w stanie natychmiast wykryć nieprawidłowości w sieci, analizując dane z milionów plików i zdarzeń. |
| 1.2 | Musi wykonywać proaktywną analizę logów i korelację zdarzeń w czasie rzeczywistym w całej infrastrukturze, aby szybko zidentyfikować ataki i wykryć naruszenia zasad. |
| 1.3 | Musi być w stanie skorelować miliony zdarzeń z sieci, systemów, aplikacji, maszyn wirtualnych i infrastruktury pamięci masowej przy użyciu funkcji korelacji w czasie rzeczywistym. |
| 1.4 | Musi przechowywać terabajty danych, logów bez konieczności zakupu dodatkowej pamięci masowej przy użyciu wysokowydajnego modelu danych o wysokiej kompresji, który powinien kompresować |

| | |
|---|---|
| | dane w stosunku co najmniej 50:1. |
| 1.5 | Musi monitorować zarówno urządzenia, jak i systemy. Na przykład, monitorowanie kontrolerów domen Windows pod kątem prób włamania, monitorowanie firewalli pod kątem skanowania portów, monitorowanie oprogramowania antywirusowego pod kątem nieusuniętych wirusów, monitorowanie serwerów proxy pod kątem podejrzanego dostępu do adresów URL, monitorowanie bazy danych SQL pod kątem zmian w tabelach itp. |
| 1.6 | Proponowane rozwiązanie musi umożliwiać uwierzytelnianie i szyfrowanie połączenia między komponentami systemu. Również logowane dane muszą być zabezpieczone szyfrowanie oraz funkcjami haszującymi. |
| 1.7 | Pomoc w tworzeniu raportów bezpieczeństwa poprzez monitorowanie naruszeń bezpieczeństwa. |
| 1.8 | Licencjonowanie musi być oparte jedynie na ilości monitorowanych urządzeń/systemów. |
| 1.9 | Musi monitorować zmiany w systemowych plikach, folderach i kluczach rejestru dla systemów Windows. |
| 1.10 | Wbudowany analizator logów serwera Apache. |
| 1.11 | Wsparcie dla mechanizmów monitorowania i zarządzania kontami uprzywilejowanymi (Privileged Access Management). |
| 1.12 | Aktualizowane na bieżąco listy niebezpiecznych adresów IP. |
| 1.13 | Licencja rozwiązania monitorującego musi obejmować obsługę minimum 100 urządzeń/systemów oraz zapewniać aktualizacje przez minimum 3 lata. |
| **2** | **Zgodność** |
| 2.1 | Proponowane rozwiązanie do monitorowania musi zapewniać zgodność ze standardami PCI, NCUA, GLBA, FISMA, SOX lub niestandardowymi zasadami organizacji. |
| **3** | **Alarmowanie i aktywne reagowanie** |
| 3.1 | Proponowane rozwiązanie monitorujące musi być w stanie wykrywać zagrożenia dzięki aktywnemu reagowaniu na informacje pochodzące z urządzeń i systemów. |
| 3.2 | Musi posiadać wiele wbudowanych reguł do natychmiastowego użycia i dostosowania do indywidualnych potrzeb. |
| 3.3 | Musi automatycznie i interaktywnie podejmować działania w celu ochrony infrastruktury poprzez kwarantannę, blokowanie, routing i kontrolowanie adresów, usług, procesów, kont (w tym również w Active Directory) i uprawnień. Oprogramowanie musi mieć możliwość automatycznego wylogowania użytkownika, restartu lub wyłączenia komputerów, restartu lub zatrzymania usług systemu Windows a także zatrzymywania procesów w systemach Linux. |

| | |
|---|---|
| **4** | **Graficzny interfejs użytkownika** |
| 4.1 | Proponowane rozwiązanie do zarządzania musi zapewniać wysokiej jakości graficzny interfejs użytkownika dostępny za pośrednictwem standardowych przeglądarek. |
| 4.2 | Musi posiadać konsolę do monitorowania zdarzeń w czasie rzeczywistym. |
| 4.3 | Musi posiadać opcje "przeciągnij i upuść" do tworzenia filtrów i reguł. |
| 4.4 | Musi ułatwiać wyszukiwanie reguł, najlepiej przy użyciu tagów lub kategorii. |
| 4.5 | Musi mieć możliwość wyświetlania zarówno oryginalnych, jak i znormalizowanych logów w tym samym interfejsie wyszukiwania. |
| 4.6 | Musi mieć widoki „Top 10” dla występujących problemów. |
| 4.7 | Konsola do zarządzania musi być dostępna lokalnie lub zdalnie. |
| 4.8 | Konsola do zarządzania musi zezwalać wielu użytkownikom na logowanie się w tym samym czasie. |
| 4.9 | Proponowane rozwiązanie musi integrować się z Active Directory w celu logowania użytkownika oraz obsługi grup. |
| 4.10 | Oprogramowanie musi szybko wskazywać nieprawidłowości w sieci. |
| 4.11 | Proponowane rozwiązanie musi być łatwe w użyciu i intuicyjne dzięki funkcjom typu „drill-down”. |
| 4.12 | Musi posiadać podgląd zdarzeń historycznych lub w czasie rzeczywistym. |
| **5** | **Raportowanie** |
| 5.1 | Proponowane rozwiązanie w zakresie monitorowania musi być w stanie szybko wygenerować raporty dotyczące zgodności. |
| 5.2 | Musi mieć wiele wbudowanych raportów (100 lub więcej) i gotowych pakietów zgodności z normami, które pomogłyby w celach audytowych. |
| 5.3 | Proponowane rozwiązanie musi umożliwiać dostosowywanie raportów przez dodawanie / usuwanie kolumn, ustawianie filtrów, określanie ram czasowych itp. |
| 5.4 | Musi mieć raporty, które pokazują informacje dotyczące wykorzystania bazy danych. |
| 5.5 | System musi być w stanie automatycznie generować i przesyłać raporty wg ustalonego harmonogramu. |
| **6** | **Wsparcie dla wielu producentów** |
| 6.1 | Proponowane rozwiązanie monitorujące nie może być specyficzne dla producenta. |
| 6.2 | Proponowane rozwiązanie musi umożliwiać tworzenie nowych alarmów od zera a także |

| | |
|---|---|
| | definiowanie wartości progowych. |
| **7** | **Wdrożenie** |
| 7.1 | Musi umożliwiać szybkie wdrożenie na popularnych hiperwizorach, takich jak VMware lub Hyper-V. |
| **8** | **Dodatkowe komponenty** |
| 8.1 | Proponowane rozwiązanie w zakresie monitorowania musi chronić wrażliwe dane poprzez wykrywanie w czasie rzeczywistym, monitorowanie i blokowanie urządzeń USB takich jak pendrive'y, kamery, telefony. |
| **9** | **Integracja** |
| 9.1 | Proponowane rozwiązanie monitorujące musi współdzielić i korelować logi i zdarzenia z rozwiązań do monitorowania sieci, rozwiązań do monitorowania aplikacji i rozwiązań do monitorowania wirtualizacji poprzez integrację współdzielenia danych. |
| 9.2 | Musi być w stanie przyjmować trapy z monitoringu sieci, monitoringu aplikacji i innych rozwiązań do monitoringu. |
| 9.3 | Musi mieć możliwość udostępniania swoich logów za pomocą protokołów syslog. |
| 9.4 | Musi posiadać gotowe funkcjonalności obsługi danych z systemu Eset Remote Administrator/Eset Protect. |
| 9.5 | Musi posiadać gotowe funkcjonalności monitorowania systemów UTM Barracuda. |
| 9.6 | Musi posiadać gotowe funkcjonalności monitorowania urządzeń sieciowych Cisco, Cisco Small Business, Dell oraz Aruba. |
| **10** | **Skalowanie** |
| 10.1 | Proponowane rozwiązanie w zakresie monitorowania musi zapewniać możliwość długoterminowego przechowywania i wyszukiwania oryginalnych logów. |
| 10.2 | Proponowane rozwiązanie musi obsługiwać opcje wielu wdrożeń - scentralizowane, rozproszone i hybrydowe wdrożenia, z opcją scentralizowanego widoku w jednej konsoli. |
| **11** | **Częstotliwość aktualizacji** |
| 11.1 | Wydawane aktualizacje produktu, min. dwa razy w roku lub częściej. |
| **12** | **Wsparcie produktu** |
| 12.1 | Wsparcie producenta 24x7x365 przez okres 3 lat. |
| 12.2 | Wsparcie przy uruchomieniu systemu w formie konsultacji telefonicznych i mailowych lub połączenia zdalnego. Zagwarantowany czas: minimalnie 24 h – maksymalnie 48 h. |

Załącznik nr 1 do SWZ
Opis Przedmiotu Umowy

**CZĘŚĆ III**

| Przedmiot zamówienia: | **Oprogramowanie do szyfrowania danych wrażliwych** |
|---|---|
| Ilość licencji: | 55 |
| Długość subskrypcji: | 1 rok |
| Możliwości programu | -256 bitowe szyfrowanie AES<br>-Szyfrowanie plików na różnych nośnikach np. pendrive'y<br>-Możliwość zaszyfrowania całego dysku twardego |
| Język | Polski |
| Obsługiwane systemy | Microsoft Windows |
| Aktualizacje | W ramach zakupionej subskrypcji udostępnione automatyczne aktualizacje oprogramowania. |
| Centralna konsola administratora | Możliwość zdalnego blokowania urządzeń bez konieczności korzystania z VPN lub tworzenia wyjątków na firewallu. |