**OPIS PRZEDMIOTU ZAMÓWIENIA**

Systemy Wspomagające

## Pakiet 1 – Analizator logów.

Przedmiotem zamówienia jest dostawa licencji na oprogramowanie analizujące logi systemowe, którego minimalne wymagania funkcjonalne zamieszczono poniżej:

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Minimalne wymagania sprzętowe i funkcjonalne** | **Wartość wymagana** | **Wartość oferowana**  (wpisać TAK/NIE) |
|  | Aplikacja umożliwia importowanie i analizowanie plików zdarzeń | TAK |  |
|  | Aplikacja obsługuje logi co najmniej z niżej wymienionych systemów operacyjnych  - system Windows  - system Linux  - system Unix  - wirtualizatory VMWare i Hyper-V | TAK |  |
|  | Aplikacja obsługuje logi co najmniej z niżej wymienionych systemów i urządzeń:  - routery i przełączniki sieciowe (w tym Cisco, Hewlett-Packard)  - urządzenia UTM (w tym Fortinet)  - bazy danych Oracle, MySQL, MSSQL  - serwery webowe  - serwery DHCP  - serwery druku  - serwery FTP  - inne źródła logów w formacie syslog | TAK |  |
|  | Aplikacja wspiera automatyczne wykrywanie hostów | TAK |  |
|  | Aplikacja pozwala na konfigurowanie własnych widżetów i widoków | TAK |  |
|  | Aplikacja umożliwia wyszukiwanie w logach za pomocą operatora logicznego, frazy, zakresów wartości, symboli wieloznacznych i wyszukiwania grupowego | TAK |  |
|  | Aplikacja umożliwia importowanie i analizowanie plików zdarzeń | TAK |  |
|  | Aplikacja umożliwia filtrowanie zdarzeń przed zapisaniem ich w bazie danych | TAK |  |
|  | Aplikacja umożliwia szyfrowanie plików archiwum logów | TAK |  |
|  | Aplikacja pozwala agregować i analizować informacje o bezpieczeństwie oraz umożliwia zarządzanie zdarzeniami (SIEM) | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą dodawanie własnych audytów zgodności | TAK |  |
|  | Aplikacja posiada wbudowane audyty zgodności NIST, PDPA, ISO 27001:2013 | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą bezagentowe zbieranie logów | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą wysyłanie notyfikacji SMS lub e-mail | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą raportowanie i audytowanie integralności plików | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą raportowanie i audytowanie AD AZURE | TAK |  |
|  | Aplikacja może działać na PostgreSQL lub na MS SQL | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą dodawanie niestandardowych raportów | TAK |  |
|  | Aplikacja posiada funkcjonalność umożliwiającą alarmowanie w czasie rzeczywistym połączeń sieciowych z adresów IP widniejących na „czarnej liście” | TAK |  |
|  | Aplikacja posiada uwierzytelnianie użytkowników zewnętrznych przez Active Directory i RADIUS Server | TAK |  |
|  | Aplikacja pozwala na eksportowanie raportów w formatach CSV, PDF | TAK |  |
|  | Aplikacja pozwala na wykonanie analizy trendów | TAK |  |
|  | Aplikacja umożliwia wykonanie polecenia/akcji w przypadku alertów | TAK |  |