**Załącznik nr 1\_ parametry techniczne dla Zadania nr 3**

**Centralny system gromadzenia i analizy logów – Serwer SYSLOG.   
Zakup i dostawa licencji razem z wdrożeniem oraz szkoleniami.**

|  |  |  |
| --- | --- | --- |
| Specyfikacja | * Rozwiązanie musi mieć niezależną specyficzna architekturę typu wirtual appliance * Rozwiażanie musi wspierać VMware EXSi 5.1 i wyższe, VMware Workstation 12 i wyższe oraz KVM * Obsługa scentralizowanego zbierania logów * Urządzenie powinno możliwość przechowywanie logów przez minimum 180 dni z przepustowością 4000 EPS dla logów syslog * Musi posiadać minimum 2 TB dysk w możliwością rozszerzenia | Wymagane parametry  TAK |
| Monitorowanie Urządzeń | * Musi mieć możliwość monitoring stanu użyteczności urządzenia, w tym procesora, pamięci, dysk twardego i pamięć NFS * Musi mieć możliwość rejestrowania statystyk i trendów w oparciu o typ logów * Musi mieć możliwość rejestrowania statystyki i trendów w oparciu o urządzenia * Musi mieć możliwość monitorowanie stanu urządzeń wysyłających logi * Musi posiadać dostosowany możliwość tworzenia własnych dashboardów i ich zawartość | TAK |
| Zarządzanie logami | * Musi obsługiwać niestandardowe zapytania lub filtry warunków dla: logów zdarzeń, logów sieci, logów konfiguracji, logów IPS, logów zagrożeń, logów bezpieczeństwa, logów sesji, logów PBR, logów NAT (w tym NAT444), logów URL, logów wysyłania BBS, logów poczty e-mail i logów FTP * Musi mieć możliwość rozróżniania poziomów logów według kolorów * Musi mieć możliwość ustawiania kombinacji filtrów według wielu warunków * Musi mieć możliwość wyszukiwania pełnotekstowego pola adresu URL * Musi mieć możliwość zapytania o zadania w tle i powiadomienia e-mail * Musi mieć możliwość utrzymania warunków zapytania * Musi mieć możliwość obsługi zapytań rozproszonych * Musi mieć możliwość wsparcia dla logów bezpieczeństwa danych * Musi mieć możliwość czytania logów IPv6: logów sesji, logów NAT, logów PBR, logów SLB, * Musi mieć możliwość wsparcia dla logów Windows | TAK |
| Raportowanie | * Statystyki obsługujące treść raportu muszą obejmować minimum zasoby systemowe, ranking ilości logów urządzeń, ranking zajętości przestrzeni logów urządzeń, ranking ilości logów, ranking całkowitej przestrzeni logów, ranking ilości logów na podstawie źródłowego adresu IP, ranking ilości logów na podstawie docelowego adresu IP, ranking trendów w dzienniku, ilość zagrożeń/ataków, dziennik sesji, dostęp do aplikacji, ranking dostępu do adresów URL itp. * Musi obsługiwać raporty okresowe według dnia, tygodnia, miesiąca, kwartału. Raporty muszę umożliwić generowanie i sortowanie według minut, godzin lub dni. * Musi mieć możliwość wysyłania raportów pocztą elektroniczną. | TAK |
| Zarządzanie systemem | * Musi mieć możliwość automatycznego czyszczenia dysku w oparciu o dostosowany próg * Musi mieć możliwość obsługi rozproszonych ustawień i architektury rozproszonej * Musi mieć możliwość obsługi funkcji NFS * Musi mieć możliwość konfiguracji zaufanego hosta * Musi mieć możliwość ustawiania automatycznego czasu letniego * Dostępu do urządzenia musi być realizowany przez interfejs Web HTTP i HTTPS oraz konfiguracji CLI przez SSH. Nie dopuszcza się używania zewnętrznych konsol i agentów w celu dostępu do urządzenia. * Musi mieć możliwość zarządzania hasłami w celu skonfigurowania minimalnej długości i złożoności hasła, maksymalnej liczby niepowodzeń logowania oraz czasu blokady po przekroczeniu maksymalnej liczby niepowodzeń logowania. * Musi mieć możliwość modyfikacji nazwy użytkownika domyślnego administratora. * System musi być dedykowanym rozwiązaniem dla oferowanego systemu Firewall i IPS w celu gromadzenia i przetwarzania logów, nie dopuszcza się realizacji funkcji systemu poprzez centralny system zarządzania * Musi mieć możliwość wykonanie kopii zapasowych logów i ustawień na serwer FTP i SFTP oraz import logów z pliku | TAK |
| Wdrożenie/obsługa | * Szkolenie dla Administratorów z konfiguracji oferowanego rozwiązania przeprowadzone przez dystrybutora oferowanego rozwiązania w języku polskim na miejscu u klienta * Oferowane rozwiązania powinny pochodzić od jednego producenta * Licencja ważna przez okres 60 miesięcy wraz ze wsparciem serwisowym nieodpłatnym. * Wdrożenie na miejscu u klienta | TAK |