# Załącznik A

**Zamawiający dopuszcza by dokumenty wymienione w Załączniku A były języku angielskim**

(bez konieczności tłumaczenia na j.polski)

**I. Ogólne wymagania zamawiającego**

1) Dostarczony sprzęt winien być fabrycznie nowy, a data produkcji nie może być wcześniejsza niż 6 miesięcy od daty dostawy. Wszystkie urządzenia, zamówione w liczbie większej niż 1 sztuka, muszą być takie same pod względem producenta/modelu/wyposażenia/koloru, muszą być wzajemnie kompatybilnie i zapewniać zamienność technologiczną. Urządzenia muszą być dostarczone w stanie wolnym od wad technicznych, prawnych i formalnych uprawnień do gwarancji i aktualizacji. Sprzęt musi zostać dostarczony oraz uruchomiony w siedzibie zamawiającego, zgodnie z jego zaleceniami.

2) Całość dostawy musi pochodzić z oficjalnego kanału dystrybucji w celu zachowania gwarancji i osiągnięciu jak najniższego czasu usunięcia usterki. Towar oferowany w ramach grup oraz wszystkie akcesoria, muszą być tego samego producenta, co dostarczany sprzęt.

Dopuszcza się dostarczenie sprzętu oraz oprogramowania o parametrach wyższych niż wskazane.

3) Gwarancja na dostarczony sprzęt musi być realizowana przez producenta sprzętu bądź partnera posiadającego autoryzację producenta. Czas gwarancji oraz naprawy urządzeń został wyszczególniony w minimalnych wymaganiach technicznych.

Wymagane dokumenty

3.1) W przypadku napraw realizowanych przez autoryzowanych partnerów, wymaga się przedstawienia dokumentów, wystawionych przez producenta sprzętu, stwierdzających fakt bycia autoryzowanym partnerem.

3.2) Wymagane jest oświadczenie producenta komputera, że w przypadku nie wywiązywania się z obowiązków gwarancyjnych oferenta lub firmy serwisującej, przejmie na siebie wszelkie zobowiązania związane z serwisem zgodnie z udzieloną gwarancją i zgodnie z wykupionymi przez Oferenta u Producenta dodatkowymi opcjami serwisowymi mającymi spełnić stawiane wymagania.

w/w dokumenty Wykonawca dostarczy przed podpisaniem umowy.

4) Zgłoszenia usterek będą przyjmowane w cyklu 24 godziny na dobę.

5) W okresie gwarancji, w przypadku braku możliwości naprawy w określonym przedziale czasowym, na czas naprawy Zamawiający wymaga nieodpłatnego wypożyczenia urządzenia, o porównywalnych parametrach umożliwiających uruchomienie konfiguracji z posiadanego urządzenia.

6) Podczas naprawy bądź wymiany urządzenia, dyski twarde i inne nośniki danych, wykorzystywane w urządzeniach, nie mogą opuścić terenu NCBJ OR POLATOM. Dopuszczalne jest wysłanie samej elektroniki z dysku magnetycznego, jako potwierdzenie uszkodzenia i nie używania nośnika przez OR POLATOM. W przypadku awarii dysku twardego, pozostaje on u Zamawiającego.

7) Wykonawca zagwarantuje wsparcie serwisowe oraz techniczne producenta. Wsparcie to musi być zapewniane poprzez dedykowany numer oraz adres email dla wsparcia technicznego i informacji produktowej. W ramach wsparcia Zamawiający będzie miał możliwość weryfikacji na stronach producenta: konfiguracji fabrycznej zakupionego sprzętu, wykupionej gwarancji oraz statusu naprawy urządzeń.

8) Wykonawca nada indywidualną numerację dla każdego z urządzeń w celu ich identyfikacji przy kontakcie z serwisem. Numeracja musi być umieszczona w widocznym dla użytkownika miejscu. Dzięki temu numerowi pracownicy działu IT będą mogli precyzyjnie przekazać serwisowi model i typ sprzętu oraz wewnętrzne dokonywać inwentaryzacji.

9) W ofercie wymagane jest podanie modelu, symbolu oraz nazwy producenta.

**II. Rozwiązanie do zbierania i analizowania logów**

1) Zamawiający wymaga, aby rozwiązanie do zbierania i analizowania logów zostało dostarczone w formie rozwiązania sprzętowego i posiadało dostęp przez interfejs web umożliwiający administratorom i operatorom wykorzystanie wszystkich funkcji. Zamawiający dopuszcza wyłącznie instalowanie usług lub aplikacji realizujących funkcjonalności obejmujące zbieranie logów z lokalizacji zdalnych oraz z systemów Windows.

1.1) Zamawiajacy wymaga aby rozwiązanie obsługiwało natywnie **co najmniej** urządzenia :

* Przełącznik HPE 2930
* Przełącznik HPE 2530
* Przełącznik HPE 5400
* Przełącznik ARUBA CX 6100
* Przełącznik ARUBA CX 6200
* Kontroler WiFi ARUBA 7010
* Wirtualizator WmVare w wersji 7
* Kontrolery KVM HP ILO
* Kontrelery KVM DELL iDrac

Wymagane dokumenty.

Wymagane jest dostarczenie z ofertą dokumentu przedstawiającego nazwy producentów, modele lub typy urządzeń obsługiwanych natywnie. Zamawiający wymaga aby na tej liście znalazły się powyżej przedstawione rozwiązania.

2) Zdarzenia z systemów Windows muszą być zbierane przez dedykowane oprogramowanie (tzw. agent) instalowane bezpośrednio na stacjach końcowych i wysyłające dane do centralnej instancji systemu.

2.1) Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików tekstowych w systemie Windows.

2.2) Agent musi zapewniać zbieranie wszystkich danych związanych ze zdarzeniem w niezmodyfikowanej formie (tzn. nie tylko części zdarzenia).

Wymagane dokumenty

2.3) Zamawiający wymaga dostarczenia dokumentacji opisującej działanie i konfigurację agenta. Dokumentację należy złożyć wraz z dostawą.

3) Oferowane rozwiązanie musi umożliwiać filtrowanie zdarzeń (przykładowo odrzucanie nieistotnych) zbieranych przez agenta Windows jeszcze przed wysłaniem do centralnej instancji. Filtrowanie zdarzeń zbieranych przez agenta Windows musi być możliwe do skonfigurowania za pomocą programowania wizualnego.

Wymagane dokumenty

3.1) Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia filtrów. Dokumentację należy złożyć wraz z dostawą.

4) Ilość agentów dla systemu Windows (Serwer) nie może być limitowana licencyjnie. Oferowane rozwiązanie musi być pozbawione limitowania pod kątem ilości zbieranych danych.

*5) Wymagania wobec Agenta Windows:*

1. dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta.
2. po zainstalowaniu, nie może wymagać interwencji administratora na systemie końcowym - musi być centralnie zarządzany, a jego konfiguracja możliwa do przeprowadzenia z poziomu interfejsu graficznego web, bez konieczności ręcznego edytowania plików systemowych. Aktualizacja konfiguracji agenta musi być automatycznie dystrybuowana bezpośrednio z centralnej konsoli systemu. Aktualizacje agenta nie mogą być przeprowadzane przy wykorzystaniu Group Policy w systemie Windows.
3. musi automatycznie tłumaczyć kody zdarzeń Windows na postać tekstową wynikającą ze zdefiniowanych słowników (przykładowo: Logon Type 2 = Interactive, Logon Type 3 = Network, etc.).
4. musi posiadać bufor lokalny na wypadek utraty połączenia stacji końcowej z centralną instancją systemu. Dane, których nie udało się przekazać do centralnej instancji systemu, muszą zostać przekazane natychmiast po powrocie połączenia, również gdy stacja robocza była w między czasie restartowana.
5. wspierać komunikację pomiędzy agentem Windows, a centralną instancją systemu musi być zaszyfrowana, min. TLS 1.2.
6. musi wspierać kolekcjonowanie nie tylko podstawowych zdarzeń z dziennika zdarzeń (Application, Security, Setup, System), ale także umożliwiać zbieranie logów z folderu Applications and Services Logs. Dodatkowo agent Windows musi umożliwiać pobieranie danych logów z plików tekstowych z systemu Windows, konfigurowane z centralnej instancji systemu, w tym możliwość wybrania ich formatu danych (przykładowo: dziennik zdarzeń, plik txt, dhcp, iis).
7. musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows.
8. musi umożliwiać zbieranie logów z płaskich plików w systemie, z którego zbierane są logi poprzez podanie ich ścieżki w systemie plików w menu konfiguracji agenta. Konfiguracja ścieżki musi uwzględniać wykorzystanie tzw. wildcardów (przykładowo: C\Windows\System32\dhcp\logs\Dhcp\*.log - pobranie wszystkich plików z wskazanego folderu zaczynających się od "Dhcp" i kończących na ".log").
9. musi istnieć możliwość zdalnego zatrzymania/uruchomienia usługi agenta na docelowym systemie - innymi słowy musi istnieć możliwość zmiany stanu odpowiedniej usługi z "Włączoną" na "Wyłączoną" i odwrotnie.
10. musi automatycznie odpytywać centralny system w zadanym interwale - tzw. heartbeat - w celu sprawdzenia czy zaszły zmiany w konfiguracji - jeżeli tak, to agent pobiera nową konfigurację, a następnie ją implementuje. Nie jest dopuszczalne "wypychanie" konfiguracji z centralnego systemu do agenta.

6) Interfejs graficzny web umożliwiający dostęp do logów, tworzenia alertów i parserów, raportów oraz zarządzania systemem musi być jednolity oraz zunifikowanym tak aby wszystkie operacje konfiguracji, zarządzania i analizy logów były w nim wykonywane.

7) Nie dopuszcza się stosowania wielu różnych interfejsów. Interfejs ten musi być dostępny z poziomu popularnych przeglądarek (przykładowo: Google Chrome, Mozilla Firefox, Opera, Microsoft Edge).

8) Stosowany w rozwiązaniu interfejs graficzny musi umożliwiać łatwe klasyfikowanie danych wejściowych (logów) na potrzeby dalszego procesowania. Klasyfikowanie powinno umożliwiać przypisywanie określonych logów do odpowiednich parserów oraz nadawanie im tagów ułatwiających dalszą pracę z logami (np. wyszukiwanie). Logika klasyfikacji powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego.

9) Oferowane rozwiązanie musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności, takich jak klasyfikacja, parsowanie, alertowanie oraz filtrowanie poprzez tak zwane programowanie wizualne, które polega na tworzeniu kodu z graficznych bloków reprezentujących określone instrukcje i funkcje na zasadach WYSIWYG.

10) Zamawiający wymaga, aby tworzenie kodu było możliwe przez osoby posiadające podstawową wiedzę programistyczną taką jak znajomość min. instrukcji warunkowych, pętli czy zmiennych, jednakże rozwiązanie musi posiadać możliwość testowania i weryfikowania poprawności logiki stworzonego kodu.

11) Oferowane rozwiązanie musi udostępniać pre-definiowane widoki danych (dashboards) podzielone na kategorie pod względem typu lub producenta urządzenia źródłowego lub aplikacji.

12) Wraz z każdą nową wersją oprogramowania zapisane widoki muszą być automatycznie aktualizowane.

*13) Wymagania ogólne wobec rozwiązania:*

1. filtrowanie nieistotnych zdarzeń na etapie klasyfikacji. Logika filtrowania powinna być tworzona przy wykorzystaniu tzw. programowania wizualnego. Wymagane jest dostarczenie dokumentacji opisującej ten proces.
2. domyślny zapis oryginalnej wersji odbieranych logów.
3. proste wyszukiwanie zapisanych w bazie logów i tworzenie raportów w formie graficznej bez konieczności wykorzystania dedykowanego języka programowania lub zapytań SQL. Wyszukiwanie i raporty muszą być integralną częścią oferowanego rozwiązania i muszą być dostępne przez interfejs graficzny web.
4. Nie dopuszcza się możliwości modyfikacji bądź manualnego usunięcia logów zapisanych w bazie. Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie.
5. Prezentowanie logów ma być realizowane w formie wykresów, zgrupowanych w tzw. widokach (dashboard). Widoki muszą być dynamicznie aktualizowane i interaktywne (tzw. "drill down" - przykładowo: wybranie wartości przedstawionej na jednym wykresie powoduje automatyczne utworzenie filtru wyszukiwania w oparciu o wybraną wartość i dostosowanie pozostałych wykresów).
6. tworzenie własnych parserów logów przy wykorzystaniu programowania wizualnego z poziomu interfejsu graficznego web. Wymagane jest dostarczenie dokumentacji zawierającej czytelną instrukcję tworzenia parserów.
7. odbieranie wszystkich rodzajów logów. W przypadku braku odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie RAW i umożliwić jego wyszukiwanie.
8. automatyczne wzbogacanie logi o tzw. metadane czyli informacje opisujące dany log (przykładowo: typ źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog) i możliwość wyszukiwania wszystkich zapisanych logów w oparciu o te dane. Metadane powinny być dodawane do logu automatycznie nawet jeżeli nie został on poddany parsowaniu.
9. posiadać wsparcie dla oprogramowania Elastic Beats - innymi słowy system musi umożliwiać zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd).

14) W procesie parsowania musi być możliwość:

1. tworzenia lub modyfikacji parsera - musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez zastosowanie jej do przykładowego logu i wyświetlenie ostatecznej wersji w jakiej log zostanie zapisany w bazie, jeżeli testowany parser zostanie użyty. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej ten proces. Dokumentację należy złożyć wraz z dostawą.

W procesie parsowania oferowane rozwiązanie musi normalizować odbierane logi do ujednoliconego formatu poprzez przypisanie poszczególnych wartości logu do odpowiadających im kluczy (format klucz = wartość). Każdy z utworzonych w procesie parsowania kluczy powinien być oddzielnie indeksowany w bazie danych aby umożliwić szybkie wyszukiwanie wartości skojarzonych z danym kluczem. Zintegrowane w systemie parsery powinny automatycznie wzbogacać procesowane logi o odpowiednią kategorię. Wymagane jest rozróżnianie przynajmniej następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji.

1. dodania w/w kategorii podczas tworzenia własnych parserów.
2. zamiany wybranych wartości logu na podstawowe typy (integer, float), w celu wykonywania na nich operacji matematycznych (suma, średnia, największa/najmniejsza wartość etc.) podczas prezentowania ich na dashboardach.
3. wykorzystania operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. Te operacje muszą umożliwiać tworzenie logiki mającej na celu tworzenie linków URL do zewnętrznych systemów oraz połączenie narzędzia z zewnętrznymi aplikacjami.
4. dodawania własnych znaczników czasu do odbieranych logów i wykorzystywać go podczas przeglądania danych. Jednocześnie system musi zachowywać oryginalny znacznik czasu z odebranych logów. Tworzenie własnych parserów musi umożliwiać ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego.
5. automatycznego wzbogacania wartości IP wyekstraktowane z pól logu o powiązany rekord DNS i dane GeoIP aby umożliwić ich graficzną reprezentację na widoku mapy świata bez konieczności wykorzystania zewnętrznych usług bądź aplikacji.
6. średnią stałą wydajność procesowania min. 2 tysięcy logów na sekundę (2000 EPS), przy założeniu średniego rozmiaru logu równego 700 Bajtów. W przypadku wystąpienia większej chwilowej ilości logów na sekundę, rozwiązanie musi być w stanie wykorzystać bufor i umożliwić odbieranie dwukrotnej większej wartości prze co najmniej 5 minut.

15) Oferowane rozwiązanie musi umożliwiać również:

1. zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze. Agent musi być centralnie zarządzany z konsoli systemu.
2. odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł.
3. procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe.
4. zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów. Proszę dostarczyć dokumentację opisującą proces konfiguracji connectora Office365.
5. monitorowanie źródeł logów i tworzenie reguł mających na celu powiadamianie administratora systemu w przypadku w którym źródło logów zdefiniowane w regule nie wyśle logów w określonym interwale. System musi być dostarczony wraz z parserami do obsługi logów generowanych przez urządzenia najpopularniejszych dostawców rozwiązań IT oraz umożliwiać tworzenie własnej logiki parsowania dla nietypowych źródeł.
6. odbieranie i procesowanie logów, zdarzeń oraz innych danych przesyłanych przez urządzenia w sposób jawny i ustandaryzowany, wykorzystując co najmniej następujące protokoły: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP RELP (szyfrowany).

Wymagane dokumenty

Wymagane jest dostarczenie schematu przepływu danych oferowanego systemu. Dokumentację należy złożyć wraz z dostawą.

1. łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu. Wymagane jest dostarczenie dokumentacji opisującej sposób tworzenia ról użytkowników.
2. wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD).
3. integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, Zamawiający wymaga również możliwości logowania lokalnego.
4. tagowanie indywidualnych źródeł danych, aplikacji, urządzeń czy całych podsieci IP, w celu oznaczania, przykładowo: lokalizacji urządzenia, jego typu, krytyczności etc. Tagi muszą być możliwe do dodania w procesie tworzenia parsera. Wszystkie dodane tagi muszą być przechowywane razem z logiem zapisanym w bazie. System musi umożliwiać filtrowanie i wyszukiwanie logów w oparciu o tagi, a także umożliwiać ograniczenie widoczności logów posiadających określony tag w procesie definiowania ról.
5. wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (Zabbix, Nagios, MRTG etc.).

Wymagane dokumenty

Wymagane jest przedstawienie kompletnej instrukcji integracji z wybranym systemem monitoringu.

1. integrację z bazami danych (przynajmniej: MSSQL, MySQL, Oracle i PostgreSQL) poprzez konektor ODBC (integracja rozumiana jako możliwości pobierania całych wierszy wybranych tabel w bazie).

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej proces konfiguracji konektora ODBC.

Dokumentację należy złożyć wraz z dostawą.

1. integrację z platformą wirtualizacji Vmware (ESXi, vSphere) poprzez dedykowany konektor pobierający logi I zdarzenia bezpośrednio z platformy.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej proces konfiguracji konektora.

Dokumentację należy złożyć wraz z dostawą.

1. weryfikację poprawności działania własnych parserów w trakcie ich pisania.
2. zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.
3. wspieranie podstawowych funkcji SIEM - tworzenie tzw. korelacji zdarzeń, umożliwiających wygenerowanie alertu w przypadku przekroczenia określonego limitu lub wystąpienia kilku zdarzeń w zdefiniowanym oknie czasowym. Tworzenie i edycja reguł korelacji musi być możliwa do przeprowadzenia za pomocą interfejsu programowania graficznego wyposażonego w funkcjonalność sprawdzania działania logiki reguły na przykładowych logach.
4. wdrożenie w trybie wysokiej dostępności, w którym możliwe jest klastrowanie przynajmniej 2 urządzeń, widzianych i zarządzanych jako pojedyncza instancja. Ustawienia klastra muszą być możliwe do skonfigurowania przez interfejs graficzny web, nie jest dopuszczalne konfigurowanie klastra poprzez ręczne modyfikowanie plików systemu operacyjnego. System musi dostarczać użytkownikom czytelnych informacji o stanie klastra i synchronizacji bazy. Wymaga się dostarczenia dokumentacji opisującej cały proces tworzenia klastra, oraz odzyskiwania danych w przypadku awarii jednego z komponentów klastra. Urządzenia pracujące w klastrze muszą przyśpieszać wyszukiwanie poprzez równoległe współdzielenie obciążenia. W przypadku pracy w trybie wysokiej dostępności, źródła wysyłające dane muszą wykorzystywać pojedynczy adres wirtualny, a klaster musi synchronizować konfigurację i odbierane logi pomiędzy urządzeniami w klastrze.
5. generowanie alertów, jeżeli w procesowanym logu zostaną spełnione zdefiniowane warunki. Alert musi być możliwy do wysłania poprzez wiadomość e-mail, a jego treść możliwa do utworzenia przez użytkownika. Oferowane rozwiązanie musi być również wyposażone w alerty i korelacje utworzone przez producenta.
6. wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail.
7. umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie programowania wizualnego. Podobnie jak w przypadku tworzenia parserów, musi istnieć możliwość weryfikacji poprawności utworzonej logiki poprzez wykorzystanie testowego logu w oknie tworzenia alertu oraz powiadamiania o ewentualnych błędach. Wymagane jest dostarczenie dokumentacji opisującej proces tworzenia i testowania poprawności alertu.
8. wysłanie logu naruszającego zdefiniowaną logikę alertu do zewnętrznych systemów, co najmniej za pomocą protokołu SMPT lub Syslog (TCP). System musi umożliwiać definiowanie własnego formatu przesyłanego logu w celu łatwiejszego dostosowania go (integracji) do systemu docelowego.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej ten proces. Dokumentację należy złożyć wraz z dostawą.

1. nadawanie alertom nowych tagów.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej sposób korzystania z gotowych tagów oraz przypisywania nowych. Dokumentację należy złożyć wraz z dostawą.

23. wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej ten proces. Dokumentację należy złożyć wraz z dostawą.

24. tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych. Tworzenie i odzyskiwanie musi być możliwe do wykonania z poziomu interfejsu graficznego web, bez konieczności tworzenia/modyfikowania skryptów, makr lub plików systemu operacyjnego.

Wymagane dokumenty

Wymagane jest dostarczenie dokumentacji opisującej ten proces.Dokumentację należy złożyć wraz z dostawą.

16) Oferowane rozwiązanie musi być dostarczone w formie urządzenia fizycznego (wszystkie elementy systemu muszą być ustawialne z interfejsu graficznego web, bez konieczności edytowania żadnych plików systemowych, skrytpów lub makr).

17) Zamawiający wymaga aby oferowane rozwiązanie gwarantowało przechowywanie danych w okresie oczekiwanej retencji aby dane były dostępne do przeszukiwania natychmiastowo, bez wprowadzania opóźnienia w postaci importu z zewnętrznych baz danych lub ich dekompresji.

18) W przypadku przeciążenia systemu logi nie mogą być tracone. Wszystkie nieobsłużone logi muszą być buforowane, a administrator systemu powiadamiany w momencie, w którym bufor zacznie się zapełniać. Bufor nie może być mniejszy nić 50GB.

19) Zamawiający wymaga aby rozwiązanie było wyposażone w dyski w systemie RAID z możliwością usunięcia jednego fizycznego dysku z systemu bez utraty danych lub wpływu na działanie systemu. Redundancja dysków nie może wpływać na wymaganą minimalną przestrzeń dyskową. System musi informować o przekroczeniu krytycznych wartości wykorzystania dostępnych zasobów sprzętowych.

20) Oferowane rozwiązanie musi bazować na urządzeniu, które będzie posiadało wszystkie komponenty niezbędne do działania (CPU, RAM, Dyski) i będzie niezależne od innych systemów.

21) Oferowane rozwiązanie musi wspierać Virtual KVM (keyboard, video, mouse). Musi wspierać zdalne zarządzanie oraz być dostarczone z licencją odpowiedniego typu (iLO, iDRAC etc).

22) Wymagania Sprzętowe

|  |  |
| --- | --- |
| Wymagania Sprzętowe |  |
| Obudowa | Rozmiar max 1U, wyposażone w ramię do kabli umożliwiające wysunięcie urządzenia z szafy rack na potrzeby serwisowe bez konieczności wyłączania.Wentylatory urządzenia muszą być wymienialne w trakcie pracy urządzenia i być redundantne skierowane ruchem przepływu powietrza front ->tył. |
| Procesor | min. 10 rdzeni wspierający HyperThreading. |
| RAM | Min. 64GB DDR-4 |
| LAN | Minimum 4 porty 1Gbit LAN + 1 dedykowany 1Gbit porty do zarządzania sprzętem. Konfiguracja parametrów wszystkich interfejsów sieciowych (w tym LACP) musi odbywać się z interfejsu graficznego web oraz musi być szczegółowo opisana w dokumentacji. |
| Zasilanie | Urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1. |
| Wydajność | Minimum 2000 zdarzeń na sekundę. |
| Pojemność bazy zebranych logów | Minimum 12 TB przestrzeni dyskowej, wspieranej przez sprzętowy akcelerator SAS RAID-5. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash. |
| RAID | Minimum 4 dyski edycji RAID do wykorzystania w warunkach data center. |
| Bufor | Minimum 50G.B |
| Gwarancja | minimum 5 lat w miejscu instalacji z gwarantowanym czasem reakcji na następny dzień roboczy od zgłoszenia, dyski pozostają u klienta. |
| System operacyjny | Zamknięty przez producenta bez możliwości połączeń SSH. Aktualizowany z konsoli administracyjnej poprzez protokół https. |
| Bezpieczeństwo | Zaszyfrowany obszar przechowywania logów. |
| Retencja danych | Minimalnie 120 dni. |

23) Wymagane dokumenty

Oferent musi dostarczyć potwierdzenie w formie certyfikatu, że oferowane rozwiązanie spełniania wymogi ISO/IEC 27001:2013 w zakresie rekordów audytowych lub równoważne.

Ww. dokument należy złożyć wraz z ofertą.

Oferent musi dostarczyć kompletną dokumentację – instrukcję obsługi oferowanego rozwiązania. Wymagane jest dostarczenie broszury szczegółowo przedstawiającej parametry techniczne oferowanego systemu. Wymaga się dostarczenia dokumentacji w formie elektronicznej lub linku do jej wersji online na stronach producenta. Nie dopuszcza się dokumentacji odnoszącej się z/do źródeł zewnętrznych, innych niż producenta.

Ww. dokumenty, tj. instrukcję obsługi oraz broszury należy złożyć wraz z ofertą.

24) Zamawiający wymaga możliwości aktualizacji systemu dystrybuowanej w formie pojedynczego pliku i instalowane za pośrednictwem interfejsu graficznego web. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta.

Wymagamy dostarczenia przynajmniej 4 ostatnich dokumentów release notes w celu zweryfikowania proponowanych parametrów systemu. System musi umożliwiać cofnięcie do poprzedniej wersji oprogramowania w przypadku wystąpienia problemów z działaniem po aktualizacji. Operacja musi być możliwa do wykonania bez wsparcia dostawcy/producenta.

Wymagane dokumenty

Zamawiajacy wymaga dostarczenia szczegółowego opisu procedury wraz z dostawą.

25) Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie, lub licencja musi umożliwiać odbieranie przynajmniej 180GB logów/dzień. System musi posiadać bazę danych o rozmiarze przynamniej 12TB oraz wspierać kompresję przechowywanych danych.

26) Wymagane wsparcie na oprogramowanie - minimum 5 lat.

27) Dostarczone rozwiązanie musi zostać dostarczone na koszt wykonawcy oraz uruchomione, a personel OR POLATOM musi zostać przeszkolony z jego obsługi. Podczas szkolenia wymaga się uruchomienia co najmniej:

* 10 źródeł z systemów Microsoft Windows przykładowo:
	+ Serwer MS SQL
	+ Serwer Exchange
	+ Serwer DHCP
	+ Serwer NPS
* 20 źródeł urządzeń przekazujących logi poprzez syslog UDP 514.
	+ 2 urządzeń firewall (jeżeli wymagane jest aby poznać nazwę producenta, model należy podpisać dokument o zachowaniu poufności)
	+ Systemu zabezpieczeń antywirusowych (jeżeli wymagane jest aby poznać nazwę producenta, model należy podpisać dokument o zachowaniu poufności)
	+ HPE
	+ ARUBA
* Mechanizm przekazywania logów o stanie Alarmowym do innego systemu w formacie syslog.