Specyfikacja techniczna przedmiotu zamówienia

Nazwa zadania: Zakup Menagera logów, czyli oprogramowanie umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z niegraniczonej liczby źródeł. W08

Parametry techniczne muszą być **<u>równoważne lub lepsze</u>** niż podane w specyfikacji.

Lp	Parametry techniczne.
1. Zakup Menagera logów, czyli oprogramowanie umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z niegraniczonej liczby źródeł. W08	**Ilość sztuk : 1** **Typ licencji na oprogramowanie:** Dożywotnia **Wdrożenie:** przez dostarczanie maszyny wirtualnej **Obsługa i pełna funkcjonalność:** przez wizualny interfejs www za pomocą przeglądarek internetowych **Wydajność (EPS):** 2000 zdarzeń na sekundę **Pojemność przechowywania:** 16 TB **Obsługa urządzeń:** Apache, Eset, ArcSight, Cisco, Dell iDrac, FlowMon, FortiAuthenticator, FortiDDoS, Fortigate, FortiMail, FortiManager, Linux, Mikrotik, Microsoft Exchange, Microsoft SharePoint, Microsoft SQL, Microsoft Windows, MySQL, Nginx, Novell eDirectory, OpenSSH server, PostgreSQL, Synology, VMware **Obsługa systemów Windows:** **-** dedykowany agent – instalacja na końcówkach - logi zbierane w oryginalnej formie (całość, nie częściowe) - nie limitowana liczba agentów - nie limitowana liczba zbieranych danych **Filtracja zdarzeń:** **-** możliwość odrzucenia nie istotnych**,** jeszcze przed wysłaniem przez agenta **-** wizualna forma konfiguracji **Wymagania Agent Windows:** **-** Dostarczanie dokumentacji - Zarządzany centralnie - Aktualizowany z konsoli centralnej - Tłumacz kodów zdarzeń na postać tekstową zdefiniowaną w słownikach - Bufor lokalny na dane, w razie braku połączenie z centralą i późniejsze ich wysłanie po odzyskaniu połączenia - Komunikacja z centralą – zaszyfrowana min TLS 1.2 - logi zbierane z systemowego dziennika zdarzeń - logi zbierane z folderów **i** plików zdefiniowanych w konsoli zarządzającej - Agent sam sprawdź dostępność swojej aktualizacji i pobiera ją z centralnego systemu - Kwalifikowanie danych wejściowych do dalszej pracy z nimi, nadawanie TAGÓW - Rozbudowa funkcjonalności - klasyfikacja , prasowanie, alterowanie, filtrowanie – funkcje na zasadach WYSIWYG - Próg wejścia programowego - podstawowy: znajomość zmiennych, instrukcji warunkowych, pętli - rozwiązanie musi posiadać możliwość testowania i weryfikowania poprawności logiki stworzonego kodu. **Wymogi ogólne:** - Filtrowanie nieistotnych zdarzeń na etapie klasyfikacji

	- Zapis oryginalnej wersji odbieranych logów - Wyszukiwanie zapisanych w bazie logów - Tworzenie raportów w formie graficznej - Każdy log ma swój identyfikator - Brak możliwość ingerencji w zapisane logi – usuwanie, modyfikacja - Tworzenie własnych parserów logów z dostarczonej dokumentacji - Prezentacja logów w formie wykresów , wykresów zgrupowanych – dynamicznie aktualizowanych - Odbieranie wszystkich rodzajów logów - Automatyczne wzbudzanie logów o metadane - źródła, protokół transportowy, port docelowy, tagi, nagłówek syslog - Zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd). **Prasowanie funkcjonalność :** **-** tworzenia lub modyfikacji parsera – weryfikacja poprawności stworzonego pasera - normalizacja logów w procesie prasowania - rozróżnianie następujących typów logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji. - Zamiany wybranych elementów logu na podstawowe typy (integer, float) - wykorzystania operacji matematycznych (dodawanie, odejmowanie, mnożenie, dzielenie) oraz operacji natywnego kodowania/dekodowania URL. - Dodawania własnych znaczników czasu do odbieranych logów - ustawienie typu wartości jako adres MAC i identyfikację producenta urządzenia sieciowego. - wzbogacania wartości IP z pól logu o powiązany rekord DNS i dane GeoIP – prezentacja na mapie świata **Funkcjonalność:** **-** Odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł - Procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe - Zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów + dokumentacja - Monitorowanie źródeł logów i tworzenie reguł, powiadomień - Odbieranie i procesowanie logów, zdarzeń oraz innych danych: UDP/TCP SYSLOG, TCP RELP (nieszyfrowany), TCP RELP (szyfrowany). - tworzenie ról definiujących poziom dostępu użytkowników - Wzbogacanie logów o dodatkowe informacje z zewnętrznych list - Integrację z systemem LDAP w celu logowania użytkowników - lokalne logowanie bez LDAP - Tagowanie indywidualnych źródeł danych - Wykorzystanie REST-API do integracji z zewnętrznymi systemami - Integrację z bazami danych (przynajmniej: MSSQL, MySQL, Oracle i PostgreSQL) - konektor ODBC - Zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259. - Wdrożenie w trybie wysokiej dostępności, klastrowanie przynajmniej 2 urządzeń. - Generowanie alertów, wysłanie przez e-mail - Wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail. - Nadawanie alertom nowych tagów. - tworzenie i odzyskiwanie kopii zapasowej konfiguracji **Dostarczona Maszyna wirtualna:** - Dostępne formaty: OVA/OVF/VHDX/VMDK

	- Maszyna wirtualna nie może posiadać dostępu zdalnego typu SSH, RDP i inne. - System operacyjny musi być zamknięty przez producenta – bez możliwości dostępu typu shell/terminal - Dostawca musi zapewnić możliwość wykonania backupu konfiguracji rozwiązania i jej odtworzenia - Działanie 24/7, odporne na restart. Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie. **Wymagane wsparcie na oprogramowanie :** 2 lata , certyfikowany ekspert Producenta **Wymóg przedłożenia ważnego certyfikatu eksperta.** **Dyski do przechowywania danych :** • **Ilość sztuk:** 5 • **Pojemność dysku:** 18TB • **Technologia:** HDD • **Interfejs:** SATA • **Prędkość obrotowa (obr./min):** 7200 • **Przepustowość Interfejsu:** 6Gb/s • **Format:** 3.5" • **Rozmiar bufora dysku pamięci:** 256 MB • **Funkcja hot-plug:** TAK • **Maks. Średnia szybkość transmisji MB/s:** 270 MB/s • **MTBF (w godz.):** 2 500 000 • **Średnie opóźnienie (ms):** 4,16 • **Stan:** Nowy , **Gwarancja producenta:** 5 lat • **Podczas składani oferty proszę podać model**

Licencje fabrycznie nowe.
Podczas składania oferty prosimy o podawanie producentów i wersji.
Sporządził: Mateusz Wieczorek

Signature Not Verified
Dokument podpisany przez Adrian Urbański;
Powiat Chodzieski
Data: 2025.06.10 13:00:18 CEST