Opis przedmiotu zamówienia dotyczący zakupu i wdrożenia analizatora 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 jego funkcji.
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.
    a) Agent Windows musi umożliwiać zbieranie logów zarówno z systemowego dziennika zdarzeń jak i z plików tekstowych w systemie Windows.
    b) Agent musi zapewniać zbieranie wszystkich danych związanych ze zdarzeniem w oryginalnej, niezmodyfikowanej formie (tzn. całość a nie tylko części zdarzenia).
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.
4. Ilość agentów dla systemu Windows nie może być limitowana licencyjnie.
   Oferowane rozwiązanie musi być pozbawione limitowania pod kątem:
   - ilości agentów,
   - liczby i wielkości zbieranych danych w skali doby (GB/dzień),
   - liczby zdarzeń na sekundę (EPS).

   Ewentualne ograniczenia architektoniczne muszą wynikać wyłącznie z wydajności oferowanego urządzenia sprzętowego i nie mogą być definiowane w modelu licencyjnym.
5. Wymagania wobec Agenta Windows:
    a) Dostarczenie dokumentacji opisującej proces instalacji i konfiguracji agenta.
    b) Musi automatycznie tłumaczyć kody zdarzeń Windows na postać tekstową wynikającą ze zdefiniowanych słowników (przykładowo: Logon Type 2 = Interactive, Logon Type 3 = Network, etc.).
    c) 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.
    d) Komunikacja pomiędzy agentem Windows, a centralną instancją systemu musi być zaszyfrowana (min. TLS 1.2).
    e) 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

f) Musi automatycznie dodawać opis tekstowy do wszystkich zbieranych zdarzeń, dokładnie tak jak jest to prezentowane w Dzienniku Zdarzeń systemu Windows.

g) 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").

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).

9. Oferowane rozwiązanie musi umożliwiać rozbudowywanie natywnie dostępnych funkcjonalności, takich jak klasyfikacja, parsowanie, alertowanie oraz filtrowanie

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

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

12. Wymagania ogólne wobec rozwiązania:

    a) Filtrowanie nieistotnych zdarzeń na etapie klasyfikacji.

    b) Zapis oryginalnej wersji odbieranych logów.

    c) 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.

    d) Każdy log musi posiadać unikalny identyfikator, który umożliwi jego jednoznaczne rozróżnienie.

    e) 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).

    f) Odbieranie wszystkich rodzajów logów. W przypadku braku odpowiedniego parsera dla odbieranego logu, system powinien zapisać go w bazie danych w formie źródłowej (RAW) i umożliwić jego wyszukiwanie.

g) 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.

h) Musi posiadać wsparcie dla oprogramowania Elastic Beats - innymi słowy system musi umożliwiać zbieranie logów wysyłanych przez agenty Beats (filebeat/winlogbeat/auditbeat/metricbeat itd).

13. W zakresie parsowania musi być możliwość:

a) Tworzenia lub modyfikacji parsera przy użyciu graficznego interfejsu webowego. System musi umożliwiać weryfikację poprawności utworzonej logiki parsera poprzez jej zastosowanie do przykładowego logu i wyświetlenie ostatecznej wersji logu, jaka zostanie zapisana w bazie danych. W przypadku wystąpienia błędów w logice parsera, system powinien poinformować o tym użytkownika w interfejsie.

b) 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 i elastyczne wyszukiwanie wartości skojarzonych z danym kluczem. System musi wspierać kategoryzację parserów oraz rozróżniać przynajmniej następujące typy logów: udane logowanie, nieudane logowanie, wylogowanie, zmiana konfiguracji.

c) Umożliwienie przypisania kategorii wymienionych w punkcie 13b podczas tworzenia własnych parserów.

d) Możliwość dodawania własnych znaczników czasu (timestamp) podczas parsowania i wykorzystywanie ich w procesie analizy danych. System musi jednocześnie przechowywać oryginalny znacznik czasu pozyskany z logu.

e) Tworzenie parserów musi umożliwiać definiowanie pól w formacie „adres MAC” wraz z identyfikacją producenta urządzenia sieciowego (na podstawie OUI).

f) System musi zapewniać średnią stałą wydajność przetwarzania nie mniejszą niż 2000 EPS (zdarzeń na sekundę) przy założeniu średniego rozmiaru logu równego 700 bajtów. W przypadku wystąpienia chwilowego wzrostu ilości logów system musi być w stanie obsłużyć dwukrotność zakładanej wartości EPS przez co najmniej 5 minut przy wykorzystaniu mechanizmu buforowania.

14. Oferowane rozwiązanie musi umożliwiać również:

a) Zbieranie logów i zdarzeń z systemów Windows poprzez dedykowanego agenta instalowanego na stacji końcowej/serwerze.

b) Odbieranie logów na przynajmniej 50 różnych portach UDP/TCP w celu ułatwienia rozróżnienia źródeł.

c) Procesowanie (kolekcjonowanie oraz parsowanie) logów z dowolnych źródeł takich jak aplikacje, systemy operacyjne oraz urządzenia sieciowe.

d) Zbieranie logów z platformy Office365 bez konieczności instalacji dodatkowych komponentów.

e) 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.

f) 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).

g) Łatwe tworzenie ról definiujących poziom dostępu użytkowników do zapisanych logów oraz poszczególnych elementów systemu.

h) Wzbogacanie logów o dodatkowe informacje z zewnętrznych list (przykład: wzbogacenie nazwy użytkownika o jego adres email i przynależność do grup AD).

i) Integrację z systemem LDAP w celu logowania użytkowników. W przypadku awarii systemu LDAP, Zamawiający wymaga również możliwości logowania lokalnego.

j) 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.

k) Wykorzystanie REST-API do integracji z zewnętrznymi systemami do monitoringu (Zabbix, Nagios, MRTG etc.).

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

m) Integrację z platformą wirtualizacji Vmware (ESXi, vSphere)

n) Weryfikację poprawności działania własnych parserów w trakcie ich pisania.

o) Zbieranie danych przynajmniej w formatach RAW, Syslog RFC5424, CEF, LEEF, JSON RFC8259.

p) 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.

q) 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..

r) Wykorzystanie pól procesowanego logu do tworzenia treści wiadomość e-mail.

s) Umożliwiać tworzenie alertów i korelacji poprzez wykorzystanie graficznego interfejsu webowego, dopuszczając zastosowanie języka typu LPQL, SQL-like lub równoważnego, o ile

konfiguracja odbywa się bezpośrednio w GUI systemu. System musi umożliwiać testowanie działania reguły korelacyjnej na przykładowych logach oraz weryfikację poprawności ich działania.

t) 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.

u) Nadawanie alertom nowych tagów.

v) Wspierać tworzenie i odzyskiwanie kopii zapasowej konfiguracji.

w) Tworzenie i odzyskiwanie kopii zapasowej bazy danych. Tworzenie kopii zapasowej musi być możliwe zarówno na żądanie jak i w określonych interwałach czasowych.

15. Oferowane rozwiązanie musi być dostarczone w formie urządzenia fizycznego spełniającego następujące wymagania:

    a) 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.

    b) Interfejsy sieciowe - 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.

    c) Zasilanie - urządzenie musi być wyposażone w 2 źródła zasilania z redundancją 1+1.

    d) Przestrzeń dyskowa - wspierana przez sprzętowy akcelerator SAS RAID-5. Kontroler macierzy dyskowej musi być wyposażony w zapasową baterię lub pamięć flash. Minimum 4 dyski edycji RAID do wykorzystania w warunkach data center. Redundancja dysków nie może wpływać na wymaganą minimalną przestrzeń dyskową. Wymagana przestrzeń składowania danych o rozmiarze przynamniej 12 TB oraz wspierać kompresję przechowywanych danych.

    e) Virtual KVM (keyboard, video, mouse) – urządzenie musi posiadać możliwość zdalnego zarządzania oraz być dostarczone z licencją odpowiedniego typu (iLO, iDRAC etc).

    f) 1 procesor (min. 10 rdzeni) wspierający HyperThreading.

    g) Min. 64GB DDR-4 RAM.

16. 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.

17. W przypadku przeciążenia systemu logi nie mogą być tracone. Wszystkie nieobsłużone logi muszą być buforowane

18. 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. Dokumenty te, tj. instrukcję obsługi oraz broszury należy złożyć wraz z ofertą.

19. Wszystkie aktualizacje muszą być możliwe do zainstalowania bez wsparcia dostawcy/producenta.
20. 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.
21. Ilość urządzeń z których zbierane są dane oraz ilość logów liczona w GB/dzień nie może być ograniczona licencyjnie, ani w zakresie parametrów EPS (Events Per Second), ani w zakresie wolumenu danych (GB/dzień), ani liczby źródeł.
22. Wymagane wsparcie na oprogramowanie - minimum 2 lata
23. Hardware - min. 5 lat gwarancji na sprzęt ze wsparciem on-site i gwarantowanym czasem odpowiedzi next business day od momentu zgłoszenia awarii.
24. Wymagane jest przedstawienie przynajmniej 3 referencji oferowanego systemu dotyczących projektów związanych z oferowanym systemem
25. Wykonawca dysponuje lub będzie dysponował w trakcie realizacji przedmiotu zamówienia zespołem składającym się z co najmniej dwóch ekspertów, w tym co najmniej jeden ekspert posiada certyfikat CISSP - Certified Information Systems Security Professional lub równoważny. Za równoważny uznaje się certyfikat wystawiany przez niezależną instytucję posiadającą uprawnienia do potwierdzania kompetencji w obszarze bezpieczeństwa systemów informatycznych. Certyfikat równoważny musi dotyczyć tego samego obszaru kwalifikacji, a jego uzyskanie musi wiązać się z przejściem procedury certyfikacyjnej takiej samej jak w przypadku certyfikatu porównywanego.

    Oraz jeden z ekspertów posiadający certyfikację poświadczający kompetencjie w obszarze wdrażania systemów Logmanagement/SIEM.
26. Dostarczone rozwiązanie musi zostać dostarczone na koszt wykonawcy oraz uruchomione, a personel musi zostać przeszkolony z jego obsługi. Wykonawca zapewni 6h szkolenie dla 2-óch osób
    1. Szkolenie odbędzie się w formie zdalnej.
    2. Szkolenie musi być prowadzone w języku polskim.
27. Wdrożenie powinno obejmować:

Podłączenie:

- 10 źródeł z systemów Microsoft Windows przykładowo:
    - Serwer Windows, Serwer AD, Kontroler Domeny, Serwer DHCP, Serwer DNS
- 40 źródeł urządzeń przekazujących logi poprzez syslog UDP 514.
    - Serwer Linux, Serwer ESX, Urządzenia sieciowe (rourery i switche),Firewalle

Skonfigurowanie:

- Zbudowanie 10 scenariuszy naruszenia bezpieczeństwa w oparciu o dostępne szablony producenta