

# Opis Przedmiotu Zamówienia dla usługi wdrożenia rozwiązania centralnego składowania dzienników w opcji Open Source

1. Wymagania związane z rozwiązaniem centralnego składowania dzienników zdarzeń:
  - 1.1. System operacyjny powinien być na licencji Open Source.
  - 1.2. Platformą sprzętowa dla rozwiązania centralnego składowania dzienników jest w sieci Zamawiającego wirtualna maszyna w środowisku Hyper-V.
  - 1.3. Architektura systemu powinna bazować na komponentach o licencjonowaniu Open Source czyli MongoDB oraz Opensearch.
  - 1.4. Aplikacja ma służyć do monitorowania i analizy danych, a jej celem jest pomoc Zamawiającemu w wykrywaniu zagrożeń i łagodzenie skutków potencjalnych ataków.
  - 1.5. Oprogramowanie sprzętowe umożliwiające zbieranie i zarządzanie logami oraz danymi maszynowymi pobranymi z nieograniczonej liczby źródeł.
  - 1.6. System ma na bieżąco kontrolować sytuację w sieci, zbierać wszystkie dane i dostarczać je bezpośrednio do użytkownika.
  - 1.7. Możliwość filtrowania logów i prezentowania wyników w formie łatwych do zrozumienia wykresów, generowania raportów, a także tworzenia alertów informujących o wystąpieniu potencjalnie szkodliwych zdarzeń.
  - 1.8. Określenie miejsca docelowego archiwum logów oraz tworzenie reguł automatycznego wyzwalania archiwum logów.
  - 1.9. Wyszukiwanie i filtrowanie logów odebranych od innych urządzeń sieciowych.
  - 1.10. Łatwy dostęp do zdarzeń z systemów plików (kontrola nad dostępem do danych).
  - 1.11. Wsparcie w procesie diagnostyki i rozwiązywania incydentów bezpieczeństwa (responsywny interfejs umożliwiający przejście od ogółu do szczegółu – „drill down”).
  - 1.12. Bezpieczeństwo przechowywania dowodów incydentów
  - 1.13. Brak ograniczeń licencyjnych.
  - 1.14. Tworzenie użytkowników w systemie centralnego składowania logów powinno odbywać się z wykorzystaniem zewnętrznego źródła tożsamości użytkowników (Active Directory) lub ręcznie przez definiowanie kont w samym rozwiązaniu.
  - 1.15. Konta użytkowników w systemie powinny podlegać regulacją pozwalającym na przypisanie ról dla poszczególnych pracowników. Wymagane jest minimalnie, aby system pozwalał na kreowanie ról dostępowych do systemu, które pozwalają na przyznawanie m.in. pełnych uprawnień do systemu, roli menadżera alarmów, operatora widoków nawigacyjnych (dashboardów).
  - 1.16. System centralnego składowania dzienników zdarzeń powinien mieć możliwość zdefiniowania dowolnie wielu i dowolnie skonfigurowanych źródeł danych, wśród których znajdują się m.in.: Sysloga UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Konfiguracja źródeł danych powinna pozwalać na zdefiniowanie dowolnego portu komunikacji, np. Syslog UDP 514 lub/i Syslog UDP 10514.
  - 1.17. System centralnego składowania dzienników zdarzeń powinien mieć możliwość ekstrakcji fragmentów wpisów logów z możliwością wykorzystania ich do filtrowania danych, budowania zapytań dla powiadomień i alarmów czy widoków w ramach dashboardów.
  - 1.18. System centralnego składowania dzienników zdarzeń powinna udostępniać możliwość budowania widoków w formie dashboardów, które w łatwy sposób można udostępnić w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV czy urządzeniach z dowolną przeglądarką WWW.

- 1.19. System centralnego składowania dzienników zdarzeń powinien pozwalać na budowanie powiadomień (alarmów) w oparciu o reguły, które uwzględniają napływające dane z dzienników systemowych w sieci Zamawiającego.
- 1.20. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia paczek składających się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe i pulpitów nawigacyjnych (dashboardów).
- 1.21. System centralnego składowania dzienników zdarzeń powinien mieć możliwość tworzenia lub importowania listy z pliku do użycia w źródłach wejściowych.
2. W zakresie wdrożenia proponowanego rozwiązania wykonawca wykona następujące czynności opisujące zarówno konfigurację rozwiązania jak i szkolenie z codziennego wykorzystania systemu centralnego składowania dzienników zdarzeń:
  - 2.1. Instalacja systemu operacyjnego na wybranych przez Zamawiającego maszynie wirtualnej.
  - 2.2. Weryfikacja źródła czasu na wszystkich urządzeniach/systemach wysyłających logi do Centralnego systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie mają wspólnego zegara czasu Wykonawca proponuje rozwiązanie pozwalające na uspołnienie zegarów czasów sieci Zamawiającego.
  - 2.3. Instalacja proponowanego rozwiązania wraz ze wstępną konfiguracją parametrów podstawowej pracy, w tym polityki dostępu dla pracowników zespołu IT Zamawiającego.
  - 2.4. Konfiguracja retencji przechowywania danych, z uwzględnieniem zapisów aktyw prawnych i dobrych praktyk występujących w środowisku Zamawiającego.
  - 2.5. Konfiguracja na urządzeniach i systemach w sieci Zamawiającego usługi wysyłania dzienników zdarzeń (logów) do wdrażanego systemu. Zamawiający wymaga, aby w zakresie minimalnym prace objęły:
    - (1x) Urządzenie klasy UTM firmy Fortigate
    - (1x) Przełącznik zarządzalny firmy Tplink
    - (3x) Przełączniki zarządzalne firmy UBNT
    - (8x) Serwery Wirtualne Windows
    - (2x) NAS firmy Qnap
    - (3x) Serwery wirtualne Linux
    - (25x) stacji roboczych Windows 10 i 11
    - (1x) Aplikację centralnego zarządzania Gdata
    - (3x) Serwer wirtualizacji HYPERV
    - (2x) Serwer hosta usług pulpitu zdalnego dla 50 użytkowników
    - (1x) Unifi Controller
    - (8x) bramka DECT Yealink
  - 2.6. Zdefiniowanie portów nasłuchu logów w oparciu o segmentację nasłuchu pozwalającej odseparować dane napływające z różnych typów urządzeń i systemów w sieci Zamawiającego.
  - 2.7. Wykonanie wstępnej analizy napływających logów w celu zdefiniowania odpowiednich ekstraktorów wydzielających wybrane segmenty danych z napływających strumieni logów.
  - 2.8. Wykonanie całkowitej rekonfiguracji rozwiązania **Axence nVision** w celu umożliwienia interakcji między rozwiązaniami, która umożliwi przesyłanie i analizę logów z wyżej wymienionego rozwiązania. Rekonfiguracja ma umożliwić pobieranie logów takich jak:
    - Aktywność Administratorów w konsoli centralnego zarządzania, z klasyfikacją wykonanych czynności;
    - Listę zdarzeń co do których nVision ogłasza alarm, z klasyfikacją na typ zdarzenia, istotność oraz źródło problemu;
  - 2.9. Automatyzacja analizy napływających logów poprzez zbudowanie Dashboardów generujących i prezentujących dane w postaci tabelarycznej i lub graficznej.

- 2.10. Konfiguracja mechanizmów alarmowania i powiadomień oparta o analizę napływających i przeanalizowanych logów.
- 2.11. Konfiguracja wysyłania powiadomień poprzez maila lub Microsoft Teams w przypadku stwierdzenia przez system niepokojącej sytuacji zgodnie z wcześniej ustawionymi alarmami.
3. Szkolenie z wdrożonego rozwiązania :
  - 3.1. Zamawiający wymaga aby Wykonawca zorganizował i przeprowadził w swojej siedzibie lub innym miejscu nie zależnym od Zamawiającego warsztaty techniczne z zarządzania i administracji wdrożonego systemu.
  - 3.2. Zamawiający wymaga aby usługa została zrealizowana w terminie do 6 miesięcy od zamówienia usługi.
  - 3.3. Zamawiający wymaga przeszkolenia w formie warsztatów 1 uczestnika.
  - 3.4. Zamawiający wymaga aby w trakcie warsztatów realizowane były ćwiczenia opisujące codzienną pracę administracyjną z wdrożonym systemem, rozwiązywaniem problemów, procedurę aktualizacji rozwiązania oraz rozbudowy o dodatkowe widoki i kanały napływu danych.
  - 3.5. Wymagana agenda warsztatów:
    - Wstęp do zarządzania logami
    - Wymagania techniczne, architektura oraz różnice w wersjach
    - Instalacja i konfiguracja ogólnych ustawień
    - Zbieranie logów, czyli konfiguracja metod pozyskiwania dzienników zdarzeń.
    - Przetwarzanie dzienników zdarzeń, czyli tworzenie strumieni logów, ich parsowanie oraz filtrowanie
    - Wizualizacja logów czyli tworzenie czytelnych zestawień tabelarycznych i graficznych
    - Konfiguracja alertów i powiadomień.
    - Administracja i utrzymanie
    - Case Study czyli praktyczne przykłady użycia
  - 3.6. Zamawiający wymaga aby warsztaty zamykały się w ramach czasowych 2 dni roboczych (2x 7 godz.)
  - 3.7. Zamawiający wymaga aby wykonawca pokrył koszty pełnego wyżywienia i zakwaterowania uczestnika w czasie warsztatów.
  - 3.8. Zamawiający wymaga aby warsztaty kończyły się potwierdzeniem uczestnictwa w formie certyfikatu.
4. Gwarancja i asysta techniczne:
  - 4.1. Zamawiający wymaga aby Wykonawca w czasie do 12 miesięcy od wdrożenia rozwiązania zapewnił wsparcie techniczne polegające na zdalnej pomocy w przypadku wystąpienia problemów z działaniem systemu.
  - 4.2. Zamawiający wymaga aby Wykonawca w okresie do 12 miesięcy od wdrożenia rozwiązania świadczył asystę w zakresie aktualizacji zarówno systemu, jak i jego komponentów.
  - 4.3. Zamawiający wymaga aby w/w usługi były świadczone od poniedziałku do piątku między godzinami 8.00 a 16.00.
  - 4.4. Zamawiający akceptuje fakt, że każda interwencja wymagać będzie od niego zgłoszenia potrzeby pomocy drogą elektroniczną, a wskazany kanał komunikacji będzie wyznaczony przez Wykonawcę, i może to być system zgłoszeń elektronicznych lub komunikacja mailowa.