



Cyberbezpieczny Samorząd

Zakup i wdrożenie oprogramowania do zbierania logów

I. Przedmiot zamówienia:

1. Przedmiotem zamówienia jest dostawa, wdrożenie oraz konfiguracja rozwiązania do centralnego zbierania, przechowywania i analizy logów z urządzeń i systemów informatycznych w infrastrukturze Zamawiającego. Rozwiązanie ma umożliwiać monitorowanie, analizę i raportowanie zdarzeń w czasie rzeczywistym oraz przechowywanie logów zgodnie z wymogami prawnymi i regulacyjnymi.
2. Wykonawca dostarczy licencje na oprogramowanie niezbędne do działania systemu, umożliwiające pełne wykorzystanie funkcjonalności opisanych w niniejszym dokumencie. Licencje muszą być ważne przez co najmniej 24 miesiące od momentu wdrożenia rozwiązania.

II. Wymagania techniczne dotyczące rozwiązania

1. Rozwiązanie powinno działać na systemie operacyjnym na licencji Open Source.
2. System centralnego składowania dzienników zdarzeń powinien być zainstalowany na fizycznym serwerze będącym na wyposażeniu Zamawiającego, wirtualnej maszynie w środowisku Hyper-V.
3. System powinien być oparty na komponentach z licencjonowaniem Open Source.
4. Zamawiający przeznaczy na potrzeby rozwiązania sprzętowego maszynę wirtualną o następujących parametrach:
 - Procesor (CPU): 8 rdzeni,
 - Pamięć RAM: 16 GB,
 - Dysk twardy (HDD): 2 TB.
5. System powinien umożliwiać tworzenie użytkowników za pomocą zewnętrznego źródła tożsamości (Active Directory) lub ręczne definiowanie kont w samym rozwiązaniu.
6. System powinien umożliwiać zdefiniowanie i skonfigurowanie dowolnej liczby źródeł danych, takich jak Syslog UDP/TCP, Plaintext UDP/TCP, RAW UDP/TCP, NetFlow UDP, JSON, Beat, CEF UDP/TCP. Powinna być dostępna opcja definiowania dowolnych portów komunikacji.
7. System powinien umożliwiać ekstrakcję fragmentów wpisów logów, które mogą być używane do filtrowania danych, tworzenia zapytań dla powiadomień i alertów, oraz budowania widoków w interfejsach.
8. System powinien umożliwiać tworzenie widoków w formie interfejsów, które mogą być udostępniane w trybie ReadOnly (tylko do odczytu) na urządzeniach z funkcją SMART-TV lub w dowolnej przeglądarce WWW.
9. System powinien pozwalać na tworzenie powiadomień (alertów) opartych na regułach uwzględniających napływające dane z dzienników systemowych.
10. System powinien umożliwiać tworzenie paczek, które będą składać się ze skonfigurowanych źródeł nasłuchu danych wejściowych, strumieni formatujących dane wejściowe oraz interfejsów.

III. Wdrożenie systemu

1. Wykonawca przeprowadzi instalację oraz pełną konfigurację systemu do zbierania logów, zapewniając jego optymalne działanie zgodnie z wymaganiami Zamawiającego.
2. Wykonawca zobowiązuje się do przeprowadzenia integracji systemu z istniejącymi urządzeniami oraz systemami Zamawiającego, takimi jak serwery, urządzenia sieciowe, stacje robocze oraz inne systemy, które generują logi.
3. Wykonawca zainstaluje system operacyjny na wybranym przez Zamawiającego maszynie wirtualnej.
4. Wykonawca zweryfikuje źródła czasu na urządzeniach i systemach wysyłających logi do systemu centralnego składowania dzienników zdarzeń. Jeśli urządzenia nie posiadają wspólnego zegara czasu, Wykonawca zaproponuje rozwiązanie uspoźniające zegary czasów w sieci Zamawiającego.
5. Wykonawca przeprowadzi instalację oraz wstępną konfigurację systemu, w tym konfigurację polityki dostępu dla pracowników zespołu IT Zamawiającego.
6. System zostanie skonfigurowany pod kątem retencji przechowywania danych zgodnie z przepisami prawnymi oraz dobrymi praktykami.





Cyberbezpieczny Samorząd

7. Wykonawca skonfiguruje urządzenia i systemy w sieci Zamawiającego do wysyłania dzienników zdarzeń (logów) do centralnego systemu składowania dzienników zdarzeń. Prace obejmą co najmniej:
 - 1 urządzenie klasy UTM firmy Fortigate,
 - 2 przełączniki zarządzalne firmy XXX,
 - 1 serwer Windows,
 - 45 stacji roboczych Windows 10 i 11,
 - 1 aplikację centralnego zarządzania ESET Endpoint Security,
8. Definiowanie portów nasłuchu: System zostanie skonfigurowany w sposób umożliwiający segmentację nasłuchu logów, aby odseparować dane napływające z różnych typów urządzeń i systemów.
9. Analiza logów i konfiguracja ekstraktorów: Wykonawca przeprowadzi wstępną analizę napływających logów i skonfiguruje ekstraktory, które będą wydzielać wybrane segmenty danych.
10. Wykonawca skonfiguruje interfejsy prezentujące dane w postaci tabelarycznej lub graficznej oraz zautomatyzuje analizę napływających logów.
11. Wykonawca skonfiguruje mechanizmy powiadamiania oraz alertowania oparte na analizie logów.
12. System zostanie skonfigurowany do wysyłania powiadomień poprzez email lub Microsoft Teams w przypadku wykrycia niepokojących sytuacji.
13. Wykonawca przeprowadzi szkolenie dla pracowników Zamawiającego z obsługi wdrożonego systemu, w zakresie obsługi nowego systemu, w tym zarządzania logami, tworzenia raportów, obsługi interfejsów oraz zarządzania alertami
14. Po zakończeniu wdrożenia, Wykonawca przeprowadzi testy systemu w obecności Zamawiającego w celu potwierdzenia spełnienia wszystkich wymagań określonych w zamówieniu. Odbiór końcowy nastąpi po pozytywnym zakończeniu testów.

