ZAŁĄCZNIK NR 1 DO SPECYFIKACJI

Załącznik nr 1 do Umowy nr …./2019

OPIS PRZEDMIOTU ZAMÓWIENIA (OPZ)

Przedmiotem zamówienia jest dostawa i wdrożenie systemu do zarządzania informacją i zdarzeniami bezpieczeństwa klasy SIEM (Security Information and Event Management) polegające na:

a) dostarczeniu licencji i wykonaniu instalacji oprogramowania,

b) przeprowadzeniu szkoleń z zakresu administracji, obsługi i utrzymania dostarczonego oprogramowania,

c) konfiguracji oprogramowania i uruchomieniu produkcyjnym,

d) świadczeniu usługi wsparcia technicznego.

zgodnie z poniższymi wymaganiami:

1. Narzędzie umożliwia zbieranie oraz przetwarzanie logów z różnych źródeł między innymi:

1.1 Baz danych – takich jak – msSQL, mySQL oraz Oracle,

1.2 Routerów oraz switch'y – minimum Cisco,

1.3 Skanerów podatności minimum Cisco IPS, IDS, PaloAlto,

1.4 Serwerów WEB działających w systemie Windows i Linux,

1.5 Wirtualizatorów – minimum HyperV i Vmware,

1.6 Urządzeń Windows, minimum Windows 10 Pro, Windows serwer 2016,

1.7 Urządzeń opartych o architekturę Linux,

1.8 Firewalli - minimum Cisco, PaloAlto,

1.9 Antywirusów – minimum Symantec.

2. Narzędzie umożliwia zbieranie danych w trybie agentowym oraz bez agentowym.
3. Narzędzie umożliwia import logów z innych źródeł.
4. **Narzędzie posiada wbudowany mechanizm, który potrafi przetworzyć niestandardowy format logu, do zestandaryzowanego formatu spełniający warunek czytelności dla człowieka zapisów w zbiorze zdarzeń, możliwość wyszukiwania, możliwy do zinterpretowania format np. Unified Logging System (ULS), Common Event Format (CEF), Universal Log Parsing and Indexing (ULPI) itp.**
5. Narzędzie potrafi zbierać oraz analizować min. 20 000 zdarzeń na sekundę dla środowiska referencyjnego o następujących parametrach:

Procesor 16 rdzeni 64 bit, 16 GB RAM, transfer dysku 38000 Mb/s, 3 TB przestrzeni dyskowej, 1Gb karta sieciowa. Jest to wymóg katalogowy. Rzeczywista wydajność będzie zależała od środowiska Zamawiającego.

6. Narzędzie musi zbierać dane z systemów Windows za pomocą protokołu WMI.
7. Narzędzie musi wspierać zbieranie logów ze wszystkich urządzeń i systemów, które przekazują informacje w formacie syslog.
8. Narzędzie umożliwia zbieranie logów dzięki protokołom – minimum UDP, TCP/IP, SNMP, FTP, SFTP, SMB, HTTP, HTTPS, FILE.
9. Narzędzie umożliwia monitorowanie integralności plików dla Windows oraz Linux.
10. Narzędzie umożliwia zarządzanie bazą danych do przechowywania zdarzeń z poziomu aplikacji.
11. Narzędzie umożliwia automatyczne kompresowanie zbieranych logów, archiwizowanie zdarzeń oraz przywracanie archiwalnych zdarzeń.
12. Narzędzie umożliwia zabezpieczenie hasłem wyeksportowanych raportów.
13. Narzędzie umożliwia używanie podwójnej autentykacji (2FA).
14. Narzędzie umożliwia definiowanie godzin biznesowych w algorytmach analizujących.
15. Narzędzie umożliwia zarządzanie grupami roboczymi dla administratorów.
16. Narzędzie umożliwia filtrację zbieranych logów.
17. Narzędzie posiada wbudowany silnik korelacji.
18. Narzędzie utrzymuje centralne repozytorium logów pobieranych z innych urządzeń i systemów oraz realizuje funkcję zarządzania informacjami związanymi z bezpieczeństwem i zdarzeniami (SIEM).
19. Na podstawie zebranych logów narzędzie przedstawia administratorom wiarygodne informacje
    na temat stanu bezpieczeństwa i wykrytych incydentów.
20. Narzędzie dostarczane jest w formie oprogramowania możliwego do zainstalowania na fizycznym urządzeniu lub w środowisku wirtualnym VMware w systemie operacyjnym Windows lub Linux.
21. Narzędzie umożliwia zarządzanie z podziałem uprawnień ze względu na role. Tożsamość użytkowników i administratorów jest weryfikowana poprzez lokalne konto oraz zewnętrzne systemy uwierzytelniania minimum Active Directory.
22. Konsola zarządzająca jest dostępna dla nielimitowanej liczby użytkowników/administratorów,
    ma postać graficznego narzędzia uruchamianego z wykorzystaniem przeglądarki Web.

23. Narzędzie przedstawia dane w postaci raportów, wykresów, definiowanych widoków.
24. Narzędzie posiada możliwość wykonywania operacji backup i restore, uruchamianych z graficznej konsoli. System posiada możliwość wykonywania archiwizacji informacji do zewnętrznych repozytoriów danych – minimum iSCSI, SAN i NAS.
25. Narzędzie umożliwia tworzenie alarmów na podstawie reguł korelacji zdarzeń z uwzględnieniem czasu powstania zdarzeń.
26. Narzędzie umożliwia korelację długotrwałych zdarzeń, umożliwia korelację zdarzeń w oparciu o informacje z okresu min 7 dni.
27. Narzędzie umożliwia tworzenie własnych reguł korelacji zdarzeń.
28. Korelacja zdarzeń odbywa się w czasie rzeczywistym i pozwala na bieżącą analizę zagrożeń zapewniając w ten sposób sprawność operacyjną bezpieczeństwa
29. Narzędzie zapewnia możliwość tworzenia nowych raportów generowanych zgodnie z kryteriami ustalonymi przez administratorów. Raporty tworzone są w formatach PDF, CSV.
30. Narzędzie zapewnia możliwość generowania raportów na bieżąco oraz zgodnie z harmonogramem wysyłania raportów email-em.
31. Architektura systemu zapewnia skalowalność, np. licencje nie ograniczają ilości procesorów czy ilości pamięci serwera, na którym uruchamiane jest Narzędzie.
32. Narzędzie umożliwia alarmowanie poprzez SMS i e-mail.
33. Oficjalnym językiem narzędzia jest minimum język angielski.
34. Narzędzie zapewnia gotowe raporty zgodności z normami prawnymi – min: RODO art. 5 (podpunkt 1b,1f,1d) i art. 32 (podpunkt 1b,1d), ISO27001.
35. System umożliwia zbiorcze audytowanie rozproszonego środowiska Active Directory, **w formie przygotowanych raportów obejmujących**:

35.1 Nieudane próby zalogowania do środowiska domenowego,
35.2 Stacje robocze,
35.3 Serwery,
35.4 Kontrolery domen,
35.5 Poprawne logowanie użytkowników wraz z pełną historią logowania,
35.6 Nieudane próby logowania na serwery oraz historię logowań,
35.7 Zmiany dokonywane na kontach użytkowników, a w szczególności:
35.7.1 Tworzenie kont,
35.7.2 Usuwanie kont,
35.7.3 Dezaktywacja kont,
35.7.4 Modyfikacja haseł,

35.7.5 Spis zablokowanych użytkowników,

35.7.6 Historie użytkowników.

35.8 Audyt zmian w grupie obiektów, w grupie bezpieczeństwa, operacje związane z tworzeniem i usuwaniem grup.

35.9 Zmiany dokonane na obiektach komputerów, a w szczególności:

35.9.1 Tworzenie kont,

35.9.2 Usuwanie kont,

35.9.3 Dezaktywacja kont,

35.9.4 Historie kont.

35.10 Audyt zmian w jednostkach organizacyjnych, a w szczególności:

35.10.1 Tworzenie OU,

35.10.2 Usuwanie OU,

35.10.3 Lista modyfikowanych OU,

35.10.4 Historie OU.

35.11 Audyt zmian w zasadach grupowych, a w szczególności:

35.11.1 Tworzenie GPO,

35.11.2 Usuwanie GPO,

35.11.3 Lista modyfikowanych GPO,

35.11.4 Historia GPO,

35.11.5 Zaawansowane zmiany w GPO.

35.12 Audyt zmian uprawnień, a w szczególności:

35.12.1 Uprawnienia dotyczące poziomu dostępu do domeny,

35.12.2 Uprawnienia zmian OU,

35.12.3 Uprawnienia zmian w kontenerach,

35.12.4 Uprawnienia zmian w GPO,

35.12.5 Uprawnienia zmian użytkowników,

35.12.6 Uprawnienia zmian grup,

35.12.7 Uprawnienia zmian komputerów,

35.12.8 Uprawnienia zmian DNS.

35.13 Zmiany w DNS.

35.14 Audyt zmian na serwerach plików, a w szczególności:

35.14.1 Windows,

35.14.2 Windows file Cluster.

35.15 Audyt zmian na serwerach członkowskich w domenie AD.

35.16 Audyt stacji roboczych.

35.17 System umożliwia wykonanie różnego rodzaju skryptów, dzięki którym zagrożenie zostaje wyeliminowane natychmiast.

35.18 System posiada alerty o przekroczonej przestrzeni dyskowej monitorowanych urządzeń.

35.19 System przechowuje zarchiwizowany zbiór logów z audytowanego środowiska i musi mieć możliwość dokładnego ustawiania czasu przeniesienia do archiwum.

35.20 System umożliwia audyt urządzeń USB dla Serwerów Windows 2016 i systemu Windows 10 pro, a w szczególności:

35.20.1 Zmiany na plikach lub folderach,

35.20.2 Odczyt danego pliku,

35.20.3 Zmiana danego pliku,

35.20.4 Kopiowane danego pliku.

35.21 System umożliwia analitykę zachowań pokazując dane sumarycznie, a w szczególności:

35.21.1 Nietypową aktywność danego użytkownika,

35.21.2 Nietypową aktywność użytkownika na serwerze,

35.21.3 Nietypową ilość prób np. logowań,

35.21.4 Nietypowe godziny logowań użytkowników,

35.21.5 Nietypowe przydzielenie zasobów dla danego użytkownika,

35.21.6 Nietypowe działania na plikach.

36. Możliwość budowania własnych raportów w oparciu o funkcjonalności systemu wraz z możliwością harmonogramowania.

36.1 Audyt wydruków z serwera wydruków raportującego w standardzie syslog.

36.2 Możliwość budowania własnych raportów zgodności z wewnętrznymi normami organizacji.

37. Wdrożenie w lokalizacji wskazanej przez Zamawiającego.

37.1 Harmonogram wdrożenia zostanie ustalony z udziałem stron w ciągu max 7 dni od podpisania umowy.

37.2 Maksymalny czas na wdrożenie 70 dni kalendarzowych od podpisania umowy.

37.3 Zamawiający gwarantuje dostęp do administratorów Zamawiającego oraz infrastruktury
z zachowaniem procedur bezpieczeństwa Zamawiającego, w terminach ustalonych w harmonogramie.

38. Szkolenie dla Administratorów w ilości 3 dni dla 6 osób w siedzibie Zamawiającego lub w lokalizacji wskazanej przez Wykonawcę, w terminie uzgodnionym z Zamawiającym nie później jednak niż w zaproponowanym terminie wdrożenia. Koszty delegacji pracowników Zamawiającego pokrywa Zamawiający.

39. Wsparcie na rozwój i utrzymanie minimum 8 godzin w miesiącu przez 1 rok od podpisania protokołu odbioru. Wykonawca gwarantuje udzielenia wsparcia telefonicznego oraz zdalnej pomocy w utrzymaniu systemu.

40. Licencja dla następującego środowiska:

40.1 400 stacji roboczych Windows 10 pro (wdrożenie min 50 stacji),

40.2 10 Linux file serwer lub równoważne (wdrożenie dla min 4 serwerów),

40.3 15 Windows file serwer 2012 i 2016 lub równoważne (wdrożenie min 6 serwerów),

40.4 10 Switch Cisco w tym (wdrożenie min 2 x 4500x, 2 x5555, 1 x catalyst 6509),

40.5 4 Exchange Serwer (wdrożenie na 4 instancjach),

40.6 4 Active Directory (wdrożenie na 4 instancjach),

40.7 4 kontrolery domeny (wdrożenie na 4 kontrolerach),

40.8 2 x Oracle 12x (wdrożenie min 1 Oracle 12x),

40.9 2 MS SQL (wdrożenie min 1 MSSQL),

40.10 4 IIS lub równoważne (wdrożenie min 2 IIS),

40.11 4 serwery Apache lub równoważne (wdrożenie minimum 2 serwery Apache),

40.12 1 serwer wydruku (wdrożenie 1 serwera wydruku),

40.13 1 serwer Symantec lub równoważny (wdrożenie 1 serwera Symantec).

41. Zamawiający zapewnia środowisko do zainstalowania rozwiązania składające się z serwera fizycznego lub adekwatne środowisko wirtualne vMware (Windows serwer 2016 lub Linux Suse).
42. Zamawiający nie dopuszcza przechowywania danych zbieranych przez system SIEM poza swoimi placówkami – niedopuszczalne jest zastosowanie zautomatyzowanych rozwiązań do przechowywania danych w chmurach publicznych i pozbawiających Zamawiającego kontroli nad miejscem przechowywania danych.
43. Sposób licencjonowania opiera się na ilości nadzorowanych urządzeń, systemów operacyjnych, aplikacji.
44. Oferowane rozwiązanie nie może być ograniczone przez łączną ilość obsługiwanych EPS czy FPS ani ilość zbieranych danych w okresie czasu. System powinien w miarę dostępności zasobów przetwarzać wszystkie zdarzenia, które do niego wpłyną – pojawienie się tzw. pików nie powinno powodować utraty danych. Ponadto nie powinno być żadnych programowych blokad dotyczących ilości zdarzeń czy blokowanych funkcjonalności.
45. Oferowane rozwiązanie nie może wymagać użycia agentów zbierających zdarzenia i przepływy sieciowe, przekaźników i stacji pośredniczących oraz oprogramowania firm trzecich. Zamawiający dopuszcza zastosowanie dedykowanych agentów dostarczanych przez producenta rozwiązania tylko w uzasadnionych przypadkach wynikających z bezpieczeństwa systemu Zamawiającego.
46. Wsparcie serwisowe w języku polskim.
47. Wszystkie funkcjonalności muszą być gotowe na dzień składania oferty.

Użyte określenia wskazujące znaki towarowe, nazwy własne, patent lub pochodzenie przedmiotu zamówienia należy odczytywać wraz z wyrazami „lub równoważne”. Zamawiający dopuszcza zastosowanie przez Wykonawcę rozwiązań równoważnych rozwiązaniom wskazanym w opisie

przedmiotu zamówienia. Wykonawca, który w ofercie powoła się na stosowanie rozwiązań równoważnych obowiązany jest wykazać, że oferowane przez niego urządzenia i rozwiązania spełniają wymagania określone przez Zamawiającego. Wykonawca oferując przedmiot równoważny do opisanego jest zobowiązany wykazać równoważność w zakresie parametrów technicznych, użytkowych, funkcjonalnych i jakościowych, które muszą być na poziomie nie niższym od parametrów wskazanych przez Zamawiającego. W sytuacji, gdy oferowane rozwiązania lub technologie równoważne nie wymagają stosowania komponentów wymienionych w specyfikacji, Wykonawca zobowiązany jest wskazać w ofercie, który z oferowanych składników realizuje funkcję wyspecyfikowane w specyfikacji.

W przypadku, gdy zaoferowane przez Wykonawcę urządzenia (elementy) równoważne nie będą właściwie współdziałać ze sprzętem i oprogramowaniem funkcjonującym u Zamawiającego lub spowoduje zakłócenia w funkcjonowaniu pracy środowiska sprzętowo-programowego u Zamawiającego, Wykonawca pokryje wszystkie koszty związane z przywróceniem i sprawnym działaniem infrastruktury sprzętowo-programowej Zamawiającego oraz na własny koszt dokona niezbędnych modyfikacji przywracających właściwe działanie środowiska sprzętowo-programowego Zamawiającego.