Załącznik nr 3 do postępowania KA-CZL-DZP.261.1.21.2023

**OPIS PRZEDMIOTU ZAMÓWIENIA**

Przedmiotem zamówienia jest wdrożenie systemu SIEM SecureVisio

Zamawiający posiada obecnie licencje SecureVisio SIEM dla 1000 obiektów chronionych. W ramach zamówienia należy wykonać produkcyjne wdrożenie systemu zgodnie z poniższymi zapisami oraz przedłużyć wsparcie producenta systemu o kolejny rok, przeprowadzić warsztaty dla administratorów oraz zapewnić opiekę powdrożeniową. Dotychczasowe licencje wygasają z dniem 31.12.2023 r.

1. **Licencje (wykaz licencji i wsparcia, którą należy dostarczyć):**

|  |  |  |
| --- | --- | --- |
| Oznaczenie producenta | Nazwa licencji producenta | Kategoria |
| SVM-1Y-1000A | SecureVisio 1 Year maintenance for 1000 Assets | Licencja na wsparcie producenta |

1. **Wdrożenie**

Szczegółowy zakres i wytyczne procesu wdrożenia systemu zawarto poniżej.

1. **Warsztaty**

Warsztaty stacjonarne dla administratorów (8 osób) zamawiającego w formacie 3x8h w siedzibie Zamawiającego i 2x8h zdalnie poprzez platformą MS Teams. Warsztaty należy zorganizować w ustalonym z Zamawiającym terminie. Sala szkoleniowa wraz z wyposażeniem (rzutnik) zostanie udostępniona w siedzibie Zamawiającego.

1. **Wsparcie powdrożeniowe**

Zamawiający wymaga zapewnienia wsparcia powdrożeniowego w formule hypercare przez 7 dni 24/7 po zakończeniu wdrożenia i 40 godzin roboczych do wykorzystania w ciągu roku (w godzinach 8-17 w dni robocze).

**Szczegółowy zakres i wytyczne procesu wdrożenia systemu**

1. Proces wdrożenia systemu powinien zostać zrealizowany zgodnie z opisanymi niżej wytycznymi, umożliwiając efektywne wdrożenie rozwiązania w okresie min. 130 dni i maks. 150 dnia od podpisania umowy.
2. Proces wdrożeniowy podzielony zostanie na 4 obszary:
3. Obszar Analizy, zakładający stworzenie elektronicznej dokumentacji organizacji wraz z podłączeniem i skonfigurowaniem mechanizmów szacowania ryzyka pod kątem kluczowych zasobów IT i procesów organizacji (budowa kontekstu organizacji);
4. Obszar Detekcji, zakładający podłączenie i konfigurację narzędzi odpowiedzialnych za wykrywanie zdarzeń i incydentów bezpieczeństwa w ramach zainstalowania modułu SIEM;
5. Obszar Analizy ma na celu identyfikację potencjalnych cyberzagrożeń oraz możliwych konsekwencji na jakie narażona jest organizacja. Zakres prac powinien uwzględniać kolejno:
6. Pracę z konsultantem (w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej);
7. Uruchomienie systemu w infrastrukturze zamawiającego, w tym:
* konsultacje w przygotowaniu infrastruktury zamawiającego do instalacji systemu,
* instalację lub import maszyny wirtualnej typu „software appliance”,
* zestawienie połączenia zdalnego,
* aktywację licencji,
* wstępną konfigurację,
* import/wprowadzenie tabeli adresacji znaczących stref bezpieczeństwa, wymaganych przez mechanizmy wykrywania (np.: sieci serwerów, sieci DMZ, sieci LAN);
1. Podłączenie głównego źródła zdarzeń opisującego komunikację sieciową, w tym:
* przekierowanie logów opisujących transmisje sieciową (traffic) z zapór sieciowych (Firewall), przełączników i bezprzewodowych punktów dostępowych WLAN na kolektor systemu,
* uruchomienie reguł wykrywania;
1. Prace audytowe, w tym:
* pasywną analizę transmisji sieciowej:

 o ruch z/do serwerów webowych i aplikacyjnych,

 o ruch z/do serwerów baz danych,

 o ruch z/do serwerów pocztowych,

 o ruch z/do kontrolerów domenowych,

 o ruch z/do serwerów usług podstawowych (m.in. DNS/NTP),

 o ruch z/do zasobów zidentyfikowanych na bazie charakterystyki i wolumenu ruchu oraz możliwości identyfikacji aplikacji,

* + konsultacje w ramach otrzymanych wyników;
	+ zebranie danych audytowych wymaganych do sporządzenia raportu;
1. Analizę podatności, w zakresie:
	* integracji po API ze wskazanym przez Zamawiającego komercyjnym skanerem Nessus Pro;
	* przygotowanie reguł priorytetów i importu krytycznych podatności;
2. Przygotowanie dynamicznego raportu audytowego w oparciu o dostępne w systemie narzędzia elektronicznej dokumentacji i szacowania ryzyka obejmującego analizę prawdopodobieństwa przełamania zabezpieczeń organizacji. Raport powinien zawierać:
	* zidentyfikowane zagrożenia oraz prawdopodobieństwo ich wystąpienia;
	* potencjalne wektory ataków dla wykrytych zagrożeń;
	* wizualizacja graficzna wykrytych źródeł zagrożeń oraz wektorów ataków;
	* rekomendacja zabezpieczeń;
	* zidentyfikowane zagrożenia związane z podatnościami oraz prawdopodobieństwo wykorzystania ich do przełamania zabezpieczeń;
3. Transfer wiedzy w formie spotkania podsumowującego, obejmujący interpretację przez analityka wyników analizy ujętej w raporcie z systemu;
4. Obszar Detekcji ma na celu uruchomienie i dostrojenie mechanizmów wykrywania zagrożeń. Zakres prac powinien uwzględniać kolejno:
5. Podłączenie (przekierowanie do systemu) źródeł zdarzeń i ich dalszą konfigurację. Kluczowe źródła zdarzeń obejmują:
	* zapory sieciowe w punkach styku z siecią Internet (Firewall brzegowy);
	* przełączniki warstwy core;
	* sieciowe systemy bezpieczeństwa dedykowane do wykrywania incydentów bezpieczeństwa (np.: Sandbox, IDP/IPS, AntySpam);
	* centralne systemy, dedykowane do kontroli złośliwego oprogramowania na stacjach końcowych/Serwerach, umożliwiające wykrywanie aktywności złośliwego oprogramowania (np.: AntyWirus, EDR);
	* kontroler domenowy oraz system zarządzania dostępem uprzywilejowanym;
	* systemy detekcji anomalii w przepływach lub zdarzeniach (np.: NBA);
	* system SIEM;
	* w przypadku niestandardowych źródeł, muszą zostać przygotowane odpowiednie parsery, pozwalające na detekcję zgodną z wbudowanymi w system regułami korelacji;
	* Tenant Microsoft 365 wraz z Azure Active Directory.
6. Adaptację reguł profilowych, pozwalających na dostosowanie zdarzeń do zasobów, których dotyczą;
7. Podłączenie reguł detekcji;
8. Podłączenie i konfiguracja mechanizmów UEBA:
	* integracja z Active Directory;
	* utworzenie profili użytkowników UBA;
	* utworzenie profili hostów EBA;
	* import reguł bezpieczeństwa UEBA, utworzenie customowych reguł bezpieczeństwa UEBA, uruchomienie procesu uczenia;
	* obserwacja i doprecyzowanie postępu uczenia maszynowego, wykluczenie/ dodanie nowych reguł zdarzeń użytkowników/ hostów;
9. Dostrojenie systemu, w tym reguł priorytetyzacji zdarzeń i incydentów, mające na celu dopasowanie czułości systemu do możliwości operacyjnych organizacji.