OPIS PRZEDMIOTU ZAMÓWIENIA

I. Przedmiotem zamówienia jest:

Świadczenie usługi SOC (Security Operation Center), polegającej na monitorowaniu, analizowaniu i reagowaniu na incydenty związane z cyberbezpieczeństwem w modelu usługowym (dostawca usługi zapewnia po swojej stronie wymaganą infrastrukturę, oprogramowanie i niezbędne zasoby) wraz z uruchomieniem i utrzymaniem systemu klasy SIEM (Security Information and Event Management), skanera podatności oraz systemu do przeciwdziałania wyciekowi danych DLP przez okres 5 miesięcy zgodnie z poniższymi wymaganiami:

II. Wymagania formalne dotyczące wykonywanej usługi:

- Posiadanie przez wykonawcę certyfikatu na zgodność działań z normą PN-EN ISO/IEC 27001 „System zarządzania bezpieczeństwem informacji" lub równoważne przez cały okres obowiązywania umowy;

- Wykonywanie usługi SOC, o której jest mowa w OPZ zgodnie z wymaganiami Ustawy z dnia 5 lipca 2018r. o krajowym systemie cyberbezpieczeństwa w zakresie wsparcia Operatorów Usług Kluczowych, rozporządzeniem Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo;

- Podejmowanie działań i procesów operacyjnych zgodnie z wymogami norm PN-EN ISO/IEC 27001 lub równoważne, PN-EN ISO 22301 lub równoważne oraz dokumentem RFC 2350 publikowanym przez organizację Internet Engineering Task Force (IETF);

III. Wymagania formalne dotyczące wykonywanej usługi wynikające z rozporządzenia ministra cyfryzacji z dnia 4 grudnia 2019 r w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo:

- Wykonawca musi posiadać, utrzymywać i aktualizować system zarządzania bezpieczeństwem informacji spełniającym wymagania Polskiej Normy PN-EN ISO/IEC 27001 lub równoważne w zakresie obejmującym co najmniej świadczone usługi;

- Wykonawca musi zapewnić ciągłość działania usługi obsługi incydentu oraz wsparcia operatora usługi kluczowej z czasem reakcji adekwatnym do charakteru usługi kluczowej;

- Wykonawca musi posiadać i udostępniać deklarację swojej polityki działania w zakresie określonym dokumentem RFC 2350.

- Wykonawca musi przez cały okres obowiązywania umowy z Zamawiającym dysponować personelem posiadający umiejętności, o których mowa w par. 1 ust. 1 pkt 4 rozporządzenia Ministra Cyfryzacji z dnia 4 grudnia 2019r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

- Wykonawca musi posiadać możliwość wykonywania identyfikacji zagrożeń w odniesieniu do systemów informacyjnych Zamawiającego;

- Wykonawca musi posiadać możliwość wykonywania wykrywania przełamania lub ominięcia zabezpieczeń systemu informacyjnego Zamawiającego, prowadzenia analizy powłamaniowej wraz z określeniem działań niezbędnych do przywrócenia sprawności systemu informacyjnego operatora usługi kluczowej;

- Wykonawca musi posiadać możliwość wykonywania zabezpieczania informacji potrzebnych do analizy powłamaniowej, pozwalających na określenie wpływu incydentu poważnego na świadczenie usługi kluczowej, w tym informacji dotyczących: rodzajów usług kluczowych, na które incydent miał wpływ, liczby użytkowników usługi kluczowej, na których incydent miał wpływ, momentu wystąpienia i wykrycia incydentu oraz czas jego trwania, zasięgu geograficznego obszaru, którego dotyczy incydent poważny, wpływu incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych, przyczyny zaistnienia incydentu i sposobu jego przebiegu oraz skutków jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe na potrzeby postępowań prowadzonych przez organy ścigania;

- Wykonawca musi dysponować prawem do wyłącznego korzystania z pomieszczenia lub zespołu pomieszczeń, w których będzie realizowana usługa SOC, a pomieszczenia te muszą posiadać odpowiedni poziom zabezpieczeń fizycznych zgodny z w/w rozporządzeniem (należy okazać certyfikaty/dokumentację).

- Wykonawca musi dysponować redundantnymi środkami łączności umożliwiającymi prawidłową i bezpieczną wymianę informacji z podmiotami, dla których świadczą usługi SOC oraz właściwym CSiRT.

- Inne wynikające z rozporządzenia.
- Wykonawca dostosuje system do wymogów prawnych stawianych przez NIS2.

IV. <u>W skład usługi będzie wchodzić:</u>

I. monitorowanie bezpieczeństwa wraz z identyfikacją niebezpiecznych zdarzeń w ramach SOC w trybie ciągłym: 24/7/365. Minimum w zakresie:

1. Monitorowania stacji roboczych oraz serwerów, urządzeń sieciowych w tym urządzeń brzegowych, systemów/aplikacji serwerowych, w tym systemów informacji medycznej, kontrolerów domeny, środowisk chmurowych wraz z aplikacjami.

2. Powiadamiania o zagrożeniach ze stacji roboczych oraz serwerów, w szczególności generowane z narzędzi ochrony,

3. Powiadamiania o dezaktywacji narzędzi bezpieczeństwa na danym hoście,

4. Powiadamiania z modułów ochrony / bezpieczeństwa urządzeń brzegowych oraz wewnętrznych urządzeń sieciowych,

5. Zdarzeń dotyczących nieudanych, wielokrotnych prób logowania dla wszystkich monitorowanych aktywów

6. Kluczowych zdarzeń (np. utworzenie konta, zmiana hasła, usunięcie konta, zmiana grupy) związanych z kontami uprzywilejowanymi dla wszystkich monitorowanych aktywów,

7. Zdarzeń sieciowych oraz systemowych (np. enumeracja, skanowanie portów i adresacji) mogących świadczyć o rekonesansie infrastruktury,

8. Zdarzeń związanych z modyfikacją mechanizmów harmonogramu w systemach operacyjnych,

9. Zdarzeń związanych z modyfikacją audytu zdarzeń / dzienników systemowych,

10. Zdarzeń dotyczących integralności plików, w szczególności zasobów sieciowych mogących świadczyć o zainfekowaniu oprogramowaniem złośliwym

11. Zdarzeń związanych z logowaniem zdalnym.

II. uruchomienie środowiska SIEM (Security Information and Event Management), systemu do przeciwdziałania wyciekowi danych DLP oraz skanera podatności;

III. Cotygodniowe raporty analizy sieci i elementów sieciowych.

IV. uruchomienie usługi Drugiej Linii Wsparcia, minimum w zakresie:

1. Analizy zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowania raportów i zaleceń poincydentalnych

2. Realizacji Scenariuszy Reakcji zgodnie z wymaganiami.

3. Przygotowania miesięcznych raportów z realizacji prac.

4. Oczekiwanej dostępności usługi Drugiej Linii Wsparcia - 8 godzin dziennie, 5 dni w tygodniu

V. środowisko, na którym realizowana jest usługa SOC oraz SIEM będzie uruchomione na dedykowanym środowisku wysokiej dostępności HA w profesjonalnym Data Center posiadającym certyfikat na zgodność z normą PN-EN ISO 9001:2015 lub równoważne oraz normą PN-EN ISO/IEC 27001 lub równoważne (wymagane spełnienie TIER minimum III),

VI. obsługa w systemie SIEM minimum 500 EPS (event per second),

VII. ilość źródeł logów: min 200, w tym serwery Windows, serwery Linux (różne dystrybucje) oraz urządzenia sieciowe, EDR. Kolektor logów musi znajdować się w infrastrukturze Zamawiającego.

VIII. zestawienie, zabezpieczenie i obsługa połączenia w relacji Zamawiający do SOC poprzez uruchomienie łącza szyfrowanej transmisji danych w technologii VPN IP SEC o minimalnej przepustowości 50/50 Mbps,

IX. realizowanie zadań - w szczególności:

a. reagowanie na podejrzenia i obsługa zidentyfikowanych incydentów,

b. analiza incydentów i ich klasyfikowanie,

c. zarządzanie incydentami,

d. raportowanie incydentów, w tym przekazywania minimum raz w tygodniu raportów zbiorczych wykrytych incydentów / zdarzeń lub informacji o ich braku,

e. przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.

f. opracowanie i obsługa scenariuszy monitorowania i reagowania,

g. SLA o notyfikacji – do 30 min. od wystąpienia incydentu,

h. minimalny gwarantowany poziom incydentu a czas reakcji:

- incydent krytyczny – do 30 min,
- incydent niekrytyczny – do 240 min,

i. klasyfikacja (poziomy) incydentów uzgadniane będą w ramach wdrożenia i opracowywania scenariuszy monitorowania i reagowania,

j. kanały komunikacji obejmujące notyfikację: e-mail i kontakt telefoniczny,

k. raportowanie incydentów poważnych w rozumieniu ustawy o Krajowym Systemie Bezpieczeństwa do CSIRT NASK do 24h,

l. skanowanie podatności – infrastruktura krytyczna oraz stacje robocze,

m. tworzenie rekomendacji bezpieczeństwa na podstawie incydentów bezpieczeństwa – dotyczących działań związanych z powstrzymaniem incydentu oraz zalecanych środkach naprawczych.

n. przeprowadzanie testów bezpieczeństwa, obejmujących automatyczne skanowanie podatności testowanego środowiska, przeprowadzone zgodnie z założeniem, że zespół testujący, przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności (należy przedstawić harmonogram min. 1 raz w roku).

o. wykonywanie manualnych testów penetracyjnych aplikacji webowych, wykonanych zgodnie ze standardem ASVS 4.x, przeprowadzanych zgodnie z założeniem że zespół testujący przystępując do realizacji testów ma wiedzę o przedmiocie testów na poziomie analogicznym jak inni jej użytkownicy. Raport z testów musi wyszczególniać zakres przeprowadzonych testów oraz

wszystkie wyniki ze szczególnym uwzględnieniem potencjalnych skutków wpływu zmaterializowania się zagrożenia, wskazanie środków które wpłyną na poprawę stanu zabezpieczenia systemu oraz szczegóły techniczne wykrytych podatności wraz z określeniem poziomu ich istotności.

p. Wykonywanie manualnego testowania bezpieczeństwa (testy penetracyjne) oraz poprawności konfiguracji kluczowej infrastruktury teleinformatycznej, w tym infrastruktury sieciowej, usług katalogowych, platformy wirtualizacyjnej, poczty e-mail itp. – o ile testy te zostały nieuwzględnione w innych grupach kwalifikacyjnych.

X. składowanie logów i dostęp w ramach zasobów dostawcy usługi, zlokalizowane w Polsce, w trybie wysokiej dostępności HA. Okres przechowania – minimum 5 miesięcy,

XI. przedstawienie analizy przedwdrożeniowej i harmonogramu realizacji,

XII. wdrożenie, uruchomienie i przekazanie systemu do eksploatacji, uruchomienie usługi – w czasie zadeklarowanym przez usługodawcę, maksymalnie do 30.05.2025,

XIII. zapewnienie wsparcia grupy projektowej i dedykowanego kierownika projektu,

XIV. Min. 30h rocznie konsultacji i szkoleń specjalistów w zakresie organizacji/dostosowania monitorowanego środowiska.

XV. W ramach analizy przedwdrożeniowej dostawca usługi przeprowadzi analizę źródeł logów oraz określi sposób ich parsowania w SIEM, przeprowadzi analizę potrzebnych i dostępnych informacji do utworzenia reguł bezpieczeństwa dla systemu SIEM, określi wykonalności scenariuszy na podstawie dostępnych danych oraz analizę potencjalnych dodatkowych scenariuszy, wstępnie określi sposób reagowania na poszczególne podejrzenia incydentów.

XVI. W ramach podłączenia źródeł logów dostawca usługi uruchomi przesyłanie logów do SIEM, przygotuje sposób podłączania źródeł i przekaże go do Zamawiającego w celu realizacji pozostałych zasobów z tego samego typu.

XVII. Dostawca usługi przeprowadzi wstępne strojenie i implementację reguł bezpieczeństwa, a rezultatem tych prac będzie działające parsowanie logów oraz zaimplementowane uzgodnione reguły. Dostawca usługi przeprowadzi strojenie systemu SIEM w celu zmniejszenia ilości fałszywych alarmów.

V. **Minimalne wymagania skanera podatności.**

1. Automatyzacja skanowania
    i. Regularne i cykliczne skanowanie infrastruktury IT.
    ii. Możliwość uruchamiania skanów po istotnej zmianie w systemie (np. aktualizacja, wdrożenie nowej funkcji).
2. Identyfikacja podatności:
    i. Wykrywanie podatności w systemach operacyjnych, aplikacjach, bazach danych, urządzeniach sieciowych.
    ii. Klasyfikacja podatności według poziomu ryzyka.
3. Raportowanie wyników:
    i. Generowanie szczegółowych raportów z identyfikowanymi podatnościami oraz zaleceniami naprawczymi.
    ii. Możliwość eksportu wyników do formatów CSV, PDF
4. Integracja z innymi systemami:
    i. Możliwość komunikacji z systemami zarządzania poprawkami w celu automatycznego tworzenia zgłoszeń.
5. Monitorowanie i śledzenie trendów:
    i. Śledzenie liczby i rodzaju podatności w czasie.
    ii. Wizualizacja wyników za pomocą wykresów i dashboardów.
6. Bezpieczeństwo:
    i. Dostęp do wyników skanów ograniczony rolami i uprawnieniami.
    ii. Szyfrowanie danych związanych ze skanowaniem.
7. Ocena ryzyka podatności uwzględnia inne czynniki niż system klasyfikacji CVSS.
8. Zamawiający winien mieć samodzielnego wglądu do systemu i możliwość tworzenia własnych skanów i raportów.
9. System nie powinien mieć limitów co do ilości wykonywanych skanów podatności.

VI. Minimalne wymagania systemu do przeciwdziałania wyciekowi danych DLP:

1. Reguły DLP muszą być egzekwowane nawet przy braku połączenia między klientem a serwerem zarządzającym

2. Brak połączenia klienta z serwerem zarządzającym musi umożliwiać lokalne przechowywanie informacji i zebranych danych do czasu ponownego połączenia

3. Serwer administracyjny musi automatycznie pobierać aktualizacje definicji kategoryzowania stron internetowych, aplikacji i rozszerzeń plików, z opcją wyłączenia automatycznego pobierania.

4. Serwer administracyjny musi umożliwiać ustawienie powiadomień dla użytkownika końcowego w przypadku złamania reguł związanych z ochroną DLP, z możliwością dostosowania grafiki, adresu e-mail i odnośnika do polityki bezpieczeństwa.

5. Administrator musi mieć możliwość wykonać audyt stacji roboczych/użytkowników w oparciu o różne czynności, takie jak uruchomione aplikacje, podłączone urządzenia, odwiedzane strony internetowe, wydrukowane dokumenty, wysyłane i odebrane wiadomości email oraz czynności na plikach.

6. Administrator musi mieć możliwość tworzenia własnych kategorii dla stron internetowych, aplikacji i typów plików.

7. Administrator musi mieć możliwość filtrowania i sortowania zebranych danych.

8. Serwer musi posiadać możliwość wysyłania alertów, przynajmniej za pośrednictwem wiadomości email.

9. Dashboardy muszą być generowane na podstawie wskazanych stacji roboczych, użytkowników lub grup w określonym przedziale czasu.

10. Serwer administracyjny musi posiadać wbudowany serwer SMTP dostarczony przez producenta oprogramowania.

11. Serwer administracyjny musi umożliwiać wykonywanie zadań kategoryzacji plików, zarówno istniejących na stacjach roboczych i zasobach sieciowych, jak i nowo powstałych na bazie już skategoryzowanych plików.

12. Serwer administracyjny musi mieć możliwość kategoryzacji plików wrażliwych na podstawie aplikacji, lokalizacji, adresu URL, formatu pliku i zawartości pliku.

13. Dla plików skategoryzowanych, wymagana jest możliwość tworzenia reguł dotyczących blokowania i zezwalania na różne operacje, takie jak zapisywanie, przenoszenie, drukowanie, wysyłanie pocztą, wysyłanie do chmury, przesyłanie komunikatorami itp.

14. Serwer administracyjny musi umożliwiać wyszukiwanie i ochronę plików w oparciu o różne kryteria, takie jak numery kart kredytowych, numer PESEL, numer dowodu osobistego, numer paszportu, wyrażenia regularne, określone ciągi znaków i numer IBAN.

15. Weryfikacja zawartości pliku musi odbywać się w czasie rzeczywistym.

16. Serwer administracyjny musi pozwalać na eksport logów do rozwiązania SIEM.

17. Konsola musi umożliwiać konfigurację/zmianę domyślnego serwera SMTP.

18. Konsola webowa musi pozwalać na weryfikację wersji zainstalowanego oprogramowania klienta, a także umożliwia aktualizację do nowej wersji lub dezaktywację tego oprogramowania.

19. System musi ochraniać pocztę e-mail, sprawdzając każdą wiadomość e-mail wysyłaną przez użytkowników.