Załącznik nr 1

Opis przedmiotu zamówienia

Usługa monitorowania Security Operations Center dla Centrum e-Zdrowia

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

1. Słownik

Skrót lub Pojęcie	Opis
Best Effort	Stan realizacji usługi, w którym zostały przekroczone ograniczenia SLA ze względu na wystąpienie zwiększonego zapotrzebowania na usługę. W przypadku przekroczenia ograniczeń SLA Wykonawca niezwłocznie poinformuje Zamawiającego o zaistniałej sytuacji.
Cyberbezpieczeństwo	Adekwatny do potrzeb stan ochrony zapewniający możliwość wykrycia oraz reagowania na zdarzenia niepożądane oraz wskazane w dokumentacji systemu zarządzania bezpieczeństwem informacji Zamawiającego.
Cyberprzestrzeń	Przestrzeń, w której następuje wymiana, gromadzenie i udostępnianie informacji za pośrednictwem komputerów oraz komunikacja między człowiekiem i komputerem.
Czas	Wszystkie wskazania w dokumencie w zakresie czasu dotyczą czasu w aktualnej strefie czasowej przyjętej jako czas urzędowy obowiązujący w Polsce.
Departament Bezpieczeństwa	Komórka organizacyjna w strukturach Zamawiającego, odpowiedzialna za bezpieczeństwo informacji.
Dzień roboczy	Od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
Incydent Bezpieczeństwa Informacji (Incydent)	Pojedyncze zdarzenie lub serię niepożądanych albo niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji.
Koordynator Wykonawcy	Osoba z ramienia Wykonawcy odpowiedzialna za podejmowanie decyzji w zakresie realizacji spełniania warunków SLA usługi oraz za kontakt z Zamawiającym. Koordynator może mieć jednego lub wielu zastępców.
Koordynator Zamawiającego	Osoba z ramienia Zamawiającego odpowiedzialna za podejmowanie decyzji w zakresie realizacji usługi. Koordynator może mieć jednego lub wielu zastępców.
KSC	Ustawa o Krajowym Systemie Cyberbezpieczeństwa z 5 lipca 2018 roku (Dz.U. 2018 poz. 1560)
Miejsce świadczenia usługi monitorowania cyberbezpieczeństwa	Miejsce świadczenia usługi Monitorowania Cyberbezpieczeństwa przez zespół Wykonawcy spełniające wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).
Pierwsza Linia Wsparcia	Pierwsza Linia Wsparcia SOC – usługa realizująca w szczególności zadania: • Monitoringu; • Identyfikacji zdarzeń; • Analizy i eliminacji najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Druga Linia Wsparcia	Druga Linia Wsparcia SOC – usługa realizująca w szczególności zadania: • Współpracy w reakcji na zdarzenia skomplikowane i nieznane; • Tworzenie Scenariuszy Reakcji na powtarzalne zdarzenia; • Nadzór nad poprawnością działania konfiguracji scenariuszy użycia; • Wykonywanie comiesięcznych sprawdzeń działania systemów monitoringu (testy funkcjonalne).
On-call	Dyżur pod telefonem, czekanie w gotowości na zgłoszenie Drugiej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Poważnym.
CTI/OSINT	Ang. Cyber Threat Inelligence/OpenSource Inteligence - narzędzia dostarczające szczegółowe informacje o technikach hakerskich, zagrożeniach, podatnościach, artefaktach lub umiejętności ich interpretowania i dekodowania oraz czynności pozwalające na pozyskanie informacji z powszechnie dostępnych źródeł umożliwiających powiększenie zakresu wiedzy na temat potencjalnych zagrożeń.
PAM	Ang. Privileged Access Management - narzędzie wspierające nadzór nad sesjami uprzywilejowanymi oraz monitorowanie i zarządzanie uprzywilejowanymi kontami
Polityka Bezpieczeństwa Informacji dla Wykonawców	Wymagania dla Wykonawcy mające na celu zapewnienie bezpieczeństwo informacji w trakcie trwania umowy.
Praca ciągła	Praca w trybie 24/7/365 dni.
PUODO	Prezes Urzędu Ochrony Danych Osobowych – organ właściwy do spraw ochrony danych osobowych na terytorium Polski, utworzony ustawą z 10 maja 2018 roku o ochronie danych osobowych. Jest również organem nadzorczym w rozumieniu ogólnego rozporządzenia o ochronie danych.
RODO	Ustawa o ochronie danych osobowych z dnia 28 maja 2018 roku uszczegółowiające wymagania Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) jest odpowiedzią na wyzwania związane ze zmieniającą się gospodarką danymi osobowymi.
SOC	Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest całodobowe monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyberzagrożenia.
Scenariusz Reakcji	Dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z: • Zestawu możliwości technicznych wykrycia zdarzenia; • Zdefiniowanych warunków wywołania zdarzenia niepożądanego;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

	• Opisu identyfikacji zdarzeń zależnych; • Instrukcji reakcji na zdarzenie; • Instrukcji uruchomienia działań korekcyjnych; • Instrukcji wykonywania działań informacyjnych; • Ogólnych i szczegółowych ścieżek eskalacyjnych.
Scenariusz użycia systemu bezpieczeństwa	Dokument opisujący zestaw zadań wymaganych do wykonania w ramach Drugiej Linii Wsparcia, w skład którego wchodzą między innymi: • Skonfigurowanie jednego lub kilku źródeł zdarzeń; • Opisanie procesu normalizacji; • Przygotowanie Scenariuszy Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
SLA	Zestaw wartości granicznych dla kluczowych wskaźników wydajności, dla których określona realizacja usługi jest wymagany w zakresie jakościowym.
System SIEM	System zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego Zamawiającego, w którym zbierane są logi z systemów poddawane korelacji w celu wykrycia Incydentów. Zamawiający posiada System SIEM – RSA NetWitness oraz Splunk.
Transfer Wiedzy	Usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia opisana w punkcie 0.
Usługa monitorowania Cyberbezpieczeństwa	Zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów Bezpieczeństwa Informacji.
Zdarzenia niepożądane	Zdarzenie mogące wskazywać na wystąpienie incydentu bezpieczeństwa w środowisku chronionym.
Zdarzenie False-Negative	Wykrycie przez dowolną Linię Wsparcia, zdarzenia nie poprawnie rozpoznanego przy zastosowaniu ustalonych i zaakceptowanych procedur bezpieczeństwa. Realizacja i rozpoznawanie zdarzeń „ False-Negative”.
Zdarzenie False-Positive	Wykrycie przez automatyczne systemy zdarzenia, które po analizie zostało uznane jako zdarzenie poprawne. W przypadku notorycznego występowania, statystycznie rozumianego jako więcej niż 100 zdarzeń „False - Positive” na 1 incydent bezpieczeństwa w miesiącu, należy uznać regułę automatyczną tworzącą takie zdarzenia jako błędną konfigurację systemu bezpieczeństwa.
Przypadek testowy	Celowe wykonanie pełnego przebiegu zdarzenia od momentu wystąpienia sytuacji niepożądanej do momentu zakończenia przetwarzania fazy analizy incydentu. Gdy jest to możliwe, obejmuje wykonanie odwracalnych kroków reakcji na incydent, sprawdzenie scenariusza end-to-end łącznie z zablokowaniem wskaźników kompromitacji w narzędziach prewencyjnych.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa

tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl

NIP: 5251575309
REGON: 001377706

2. Przedmiot zamówienia

2.1. Przedmiotem zamówienia jest zapewnienie Usługi monitorowania Security Operations Center wraz z utrzymaniem systemu zarządzania informacjami i zdarzeniami bezpieczeństwa informatycznego (System SIEM) dla Centrum e-Zdrowia.

3. Termin realizacji oraz miejsce świadczenia Usługi

3.1. Świadczenie Usługi rozpoczęte zostanie w terminie określonym w ofercie Wykonawcy, lecz nie później niż w ciągu 30 dni (zgodnie z Ofertą Wykonawcy) od zawarcia umowy i będzie trwało przez okres 24 miesięcy (zamówienie gwarantowane).

3.2. Zamawiający może zlecić świadczenie Usługi przez okres kolejnych 12 miesięcy (zamówienie opcjonalne).

3.3. Czas, o którym mowa w pkt 3.1 – od podpisania umowy do rozpoczęcia świadczenia usługi, traktuje się jako okres przejściowy, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie dopasowanie i uzgodnienie zasad współpracy wskazanego Systemu SIEM Zamawiającego z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.

3.4. Wykonawca gwarantuje, że miejsce świadczenia Usługi wskazane w ofercie spełnia wymagania ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. 2018 poz. 1560).

3.5. Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia udostępnione przez Zamawiającego – System SIEM. Dostęp do narzędzi powinien zostać zrealizowany za pomocą szyfrowanego połączenia oraz systemu klasy PAM nagrywającego sesje osoby łączącej się, Parametry dostępu zostaną ustalone po podpisaniu umowy.

4. Wymagania dla Usługi monitorowania Security Operations Center.

4.1. Pierwsza i Druga Linia Wsparcia

W ramach realizacji zamówienia, Wykonawca będzie świadczył usługę monitorowania i analizy danych prezentowanych w Systemie SIEM zgodnie z opisanymi poniżej wymaganiami.

4.1.1. Pierwsza Linia Wsparcia

W ramach realizacji zadań Pierwszej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

(1) Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa w trybie 24 / 7 / 365, zgodnie z określonymi warunkami SLA.

(2) Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.

(3) Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji, w tym np.: uzupełnienie pliku TXT o adresy IP blokowane na urządzeniach brzegowych.

(4) Łączenie (korelowanie) zdarzeń i incydentów cyberbezpieczeństwa.

(5) Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszy Reakcji.

(6) Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.

(7) Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).

(8) Priorytetyzowanie i kategoryzowanie zdarzeń bezpieczeństwa.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

(9) Przygotowywanie dziennych raportów wykrytych zdarzeń bezpieczeństwa.

4.1.2.Druga Linia Wsparcia

W ramach realizacji zadań Drugiej Linii Wsparcia Wykonawca będzie odpowiedzialny za:

(1) Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA.
(2) Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
(3) Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
(4) Przygotowanie Scenariuszy Reakcji.
(5) Przygotowanie Miesięcznych raportów z realizacji prac.

4.2. Scenariusze

4.2.1.Scenariusz użycia systemu bezpieczeństwa

Zamawiający wymaga przygotowania i wdrożenia do 50 scenariuszy użycia dla zidentyfikowanych ryzyk przez Zamawiającego. Harmonogram wdrożenia zostanie ustalony w okresie przejściowym dla pierwszych 10 scenariuszy użycia, pozostałe scenariusze zostaną przygotowane zgodnie z pkt 7 Ogólne warunki SLA. Każdorazowo Scenariusz użycia musi zostać zaakceptowany przez Zamawiającego. Zamawiający posiada listę przykładowych scenariuszy użycia, które należy przygotować i wdrożyć. Przykładowe scenariusz użycia:

- Wykrywanie logowania z ominięciem systemu klasy PAM
- Wykrywanie utworzenia użytkownika (lokalnego i domenowego)
- Wykrycie złośliwego oprogramowania na chronionym obiekcie

4.2.1.1. Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia sytemu bezpieczeństwa zawiera:

- Skonfigurowanie jednego lub kilku źródeł zdarzeń,
- Opisanie procesu normalizacji,
- Stworzenie reguł korelacyjnych w systemie SIEM mających na celu analizowanie w referencji do listy i/lub pól wyliczeniowych i/lub analizy statystycznej, lub w inny sposób mający ujawnić incydent bezpieczeństwa,
- Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia,
- Opisanie szczegółowej ścieżki eskalacji,

4.2.1.2. Opracowanie scenariusza manualnego lub automatycznego sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia sytemu bezpieczeństwa.

4.2.2.Scenariusz Reakcji

Przygotowany przez Wykonawcę oraz zatwierdzony przez Zamawiającego Scenariusz Reakcji określa minimalny zestaw czynności konieczny do udokumentowania oraz wyciagnięcia

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

powtarzalnych wniosków, na podstawie których zostaną podjęte określone czynności. Scenariusz Reakcji składa się z podzadań realizujących funkcje:

- **Wzbogacenia** wiedzy o artefaktach tj. adresy IP, domeny, hash'e plików, nazwy plików, rozpoznawalność wskaźników kompromitacji przez narzędzia klasy CTI / OSINT, w celu wyciągania adekwatnych wniosków i podejmowania trafnych decyzji,
- **Analizy** zidentyfikowanego zdarzenia, w tym w szczególności potwierdzenia, że zagrożenie w przypadku uruchomienia w środowisku Zamawiającego może stać się incydentem lub jest incydentem, jak również rozpoczęcia pobierania lub zabezpieczenia dodatkowych danych z zaatakowanego źródła ataku zasobu na potrzeby realizacji Pierwszej Linii Wsparcia,
- **Reakcji** rozumianej jako ograniczenie możliwości wystąpienia zdarzenia niepożądanego, uruchomienia procesu eskalacyjnego lub innych czynności stosownych do zagrożenia w zakresie uzgodnionym z Zamawiającym,
- **Informowania i raportowania** obejmującego dokumentowanie wykonanych czynności oraz rezultatów przeprowadzonej analizy lub zasadności czynności reakcji.

4.3. Raport Poincydentalny

4.3.1. Zamawiający wymaga przygotowania Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 2 dni roboczych od zakończenia realizacji zawierającego informacje:

- Unikalny identyfikator zdarzenia
- Kiedy incydent wystąpił?
- Kiedy incydent został zauważony / wykryty?
- Kto lub jaki proces był sprawcą incydentu?
- Co się wydarzyło?
- Gdzie wydarzenie miało miejsce?
- Dlaczego zdarzenie mogło wystąpić?
- Jakie czynności zostały przeprowadzone w celu powstrzymania incydentu?
- Zalecenia Poincydentalne zawierające informację jakie zabezpieczenia zostały ustanowione lub powinny zostać ustanowione w celu zapobieżenia ponownemu wystąpieniu incydentu.

4.3.2. W przypadku przygotowania zaleceń, dla których konieczne jest wprowadzenie istotnych zmian do systemów bezpieczeństwa lub jakiejkolwiek rekonfiguracji systemów Zamawiającego Koordynator Wykonawcy przedstawi do akceptacji Koordynatorowi Zamawiającego zakres i szczegółową listę zmian. Zwolnione z takiej czynności są Zalecenia Poincydentalne konieczne do powstrzymania zidentyfikowanego Incydentu zagrażającego cyberbezpieczeństwu infrastruktury lub danych Zamawiającego.

4.4. Systemy Zamawiającego wymagające monitorowania

4.4.1. Usługa monitorowania, będąca przedmiotem zamówienia, w szczególności będzie obejmowała logi/dane z poniższych systemów Zamawiającego (źródło logów):

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

Rodzaj usługi lub urządzenia	Liczba urządzeń / nodów będących źródłami logów
Active Directory (liczba serwerów)	8
Windows Server	100
Linux Server SUSE	6
Linux Server CENTOS / REDHAT / ORACLE	850
DNS	10
Systemy bezpieczeństwa np.: serwer systemu antywirusowego, web application firewall, inne	20
Centralny Firewall	6
Pomocniczy Firewall	8
IPS / IDS	6
VPN	6
Routers/Switches	100

4.4.2. Zamawiający na bieżąco będzie aktualizował listę źródeł logów Zamawiającego wysyłających dane do systemu SIEM RSA NetWitness, korzysta też z SIEM Splunk w pewnym zakresie.

5. Utrzymanie systemu SIEM

5.1. Administracja Systemem SIEM:

W ramach realizacji zadań administracji Systemem SIEM Wykonawca będzie odpowiedzialny za:

5.1.1. Informowanie Zamawiającego o awariach Systemu SIEM, mogących uniemożliwić poprawne działanie systemów informacyjnych Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie,

5.1.2. Rekomendowanie zmiany zasobów takich jak: vCPU, vRAM, pamięć masowa

5.1.3. Optymalizowanie konfiguracji Systemu SIEM w celu nieprzekraczania wartości licencji Systemu posiadanego przez Zamawiającego oraz niezwłocznego zgłaszania sytuacji przekroczenia poziomu utylizacji licencji.

5.1.4. Konfigurację Systemu SIEM w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego zgodnie z punktem 4.4

5.1.5. Weryfikację czy wskazane źródła logów są poprawnie skonfigurowane w systemie - tygodniowo

5.1.6. Weryfikację czy System SIEM prawidło analizuje logi

5.1.7. Konfigurację Systemu SIEM tak aby była możliwość przeglądania do dwóch lat wstecz źródłowych zdarzeń bezpieczeństwa w zakresie:

- Logowania interakcyjne,
- Tworzenia oraz usuwania kont
- Tworzenia oraz usuwania grup użytkowników,
- Alertów źródłowych powiązanych ze zidentyfikowanymi incydentami

5.1.8. Tworzenie wymagań dla systemów Zamawiającego wysyłających logi zgodnie z punktem 4.4.1 w zakresie poziomu logowania zdarzeń.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

5.2. Testowanie Systemu SIEM:

W ramach realizacji zadań testowania Systemu SIEM Wykonawca będzie odpowiedzialny za:

5.2.1. Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu SIEM,

5.2.2. Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,

5.2.3. Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

5.2.4. Potwierdzenie co najmniej raz w miesiącu działania wszystkich wdrożonych reguł, dla wszystkich zaimplementowanych scenariuszy w ustalonym przedziale czasowym.

6. Analiza złośliwego oprogramowania

6.1.1. W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, w tym z wykorzystaniem technik inżynierii odwrotnej (ang. reverse engineering), w wymiarze zgodnym z ofertą, jednak nie mniejszym niż 12 i nie większym niż 15 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.

6.1.2. Zakres analizy złośliwego oprogramowania będzie nie mniejszy niż:

- Analiza statyczna wskazanej próbki złośliwego oprogramowania,
- Analizy dynamiczna w kontrolowanym środowisku pozwalającym na wyłączenie funkcji ukrywania lub wykrywania analizy,
- Proces odwrotny do obfuskacji umożliwiający analizę kodu zaciemnionego,
- Analiza występowania modułów pozwalających na kontrolę w tym szczegółowego określenia zaimplementowanych funkcji,
- W przypadku wykorzystywania rodziny malware określenia wersji

6.1.3. Każdorazowo po wykonanej analizie złośliwego oprogramowania Wykonawca przekaże drogą mailową raport z wykonanej analizy. Zakres raportu zostanie ustalony po podpisaniu umowy.

7. Ogólne warunki SLA

7.1. Wykonawca zapewni świadczenie Usługi monitorowania Cyberbezpieczeństwa zgodnie z określonym poziomem SLA.

<table>
<tr><th>Nazwa usługi</th><th>Poziom świadczonej usługi</th></tr>
<tr><td>Pierwsza Linia Wsparcia
Czasy dla pierwszych Incydentów każdego dnia w wymiarze zgodnym z ofertą, jednak nie mniej niż 50 i nie więcej niż 75, pozostałe zadania realizowane w trybie „Best Effort”</td><td>Dostępność usługi w trybie 24/7/365

<table>
<tr><td rowspan="2">Priorytet incydentu</td><td colspan="2">Czas od wykrycia do</td></tr>
<tr><td>Podjęcia</td><td>Realizacji</td></tr>
<tr><td>Poważny</td><td>15 min</td><td>2 h</td></tr>
<tr><td>Wysoki</td><td>60 min</td><td>6 h</td></tr>
<tr><td>Średni</td><td>2 h</td><td>12 h</td></tr>
<tr><td>Niski</td><td>4 h</td><td>24 h</td></tr>
</table>
</td></tr>
</table>

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

<table>
<tr>
<td>Druga Linia Wsparcia
Czasy dla pierwszych Incydentów każdego dnia w wymiarze zgodnym z ofertą, jednak nie mniej niż 5 i nie więcej niż 10, pozostałe zadania realizowane w trybie „Best Effort”</td>
<td>Dostępność usługi w dni robocze pomiędzy godzinami 7:00 a 18:00.
Dodatkowo dla Incydentów o priorytecie Poważnym - w trybie „on-call”:

w dni robocze w godzinach 00:00 do 7:00 i 18:00 do 24:00
w pozostałe dni w trybie „on-call” w godzinach 00:00 do 23:59

<table>
<tr><td rowspan="2">Priorytet incydentu</td><td colspan="2">Czas od eskalacji pierwszej linii wsparcia do</td></tr>
<tr><td>Podjęcia</td><td>Realizacji</td></tr>
<tr><td>Poważny</td><td>30 min</td><td>24 h</td></tr>
<tr><td>Wysoki</td><td>60 min</td><td>2 dni</td></tr>
<tr><td>Średni</td><td>2 h</td><td>4 dni</td></tr>
</table>
</td>
</tr>
<tr>
<td>Utrzymanie systemu SIEM</td>
<td>

Dostępność usługi w dni robocze w godzinach 8:00 – 16:00
Monitorowanie w ciągu tygodnia przynajmniej na poziomie 98% poprawnie skonfigurowanych urządzeń, o których mowa w pkt 4.4.1

</td>
</tr>
<tr>
<td>Analiza złośliwego oprogramowania</td>
<td>Przeprowadzenie analizy w terminie do 2 dni roboczych od przekazania podejrzanej próbki oprogramowania przez Koordynatora Zamawiającego do Koordynatora Wykonawcy oraz potwierdzenia otrzymania próbki przez Koordynatora Wykonawcy.</td>
</tr>
<tr>
<td>Scenariusz użycia systemu bezpieczeństwa</td>
<td>Przygotowanie i wdrożenie scenariusza użycia systemu wraz ze scenariuszami reakcji w terminie do 5 dni roboczych od przekazania informacji od Koordynatora Zamawiającego do Koordynatora Wykonawcy z wyjątkiem scenariuszy ujętych w harmonogramie przygotowanym w okresie przejściowym.</td>
</tr>
</table>

7.2. Oczekiwany poziom świadczenia usługi SLA dla Pierwszej i Drugiej Linii wsparcia to 98% w ciągu dnia. W przypadku niedotrzymania warunków SLA, zostaną naliczone kary umowne zgodnie z zapisami umowy.

7.3. W uzasadnionych przypadkach Wykonawca ma prawo zwrócenia się do Zamawiającego o zgodę na zawieszenie SLA na usługę Pierwszej i Drugiej Linii Wsparcia na uzgodniony z Zamawiającym okres jednak nie dłuższy niż 14 dni. Wniosek o zawieszenie SLA musi zawierać uzasadnienie. Zamawiający w takim przypadku zobowiązany jest do rozpatrzenia prośby w ciągu 1 dnia roboczego od chwili uzyskania informacji o tym fakcie. W przypadku odmowy Zamawiający jest

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

zobowiązany w ciągu 3 Dni Roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.

7.4. Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia w logach systemu komputerowego a czasem zweryfikowania poprawności nadania priorytetu.

7.5. Czas realizacji Incydentu będzie jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.

7.6. Zamawiający wyróżnia cztery poziomy incydentów: Poważny, Wysoki, Średni, Niski. Domyślnie każdy incydent zarejestrowany, jeżeli nie zostanie to uszczegółowione inaczej ma priorytet Średni.

Priorytet	Opis
Poważny	• Priorytet jest stosowany wyłącznie w przypadku wystąpienia na wskazanych zasobach lub zasobie mogącym przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO; • Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika; • Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania (C&C) trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszonego w ramach inicjatywy Trusted Introducers; • Potwierdzona informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na ustanowienie tylnej furtki, podsłuchiwanie transmisji lub wykorzystanie podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, przesłanie na dyski webowe lub danych z wykorzystaniem nieautoryzowanych nośników przenośnych; • Wykrycie przez system antywirusowy oprogramowania złośliwego na zasobie realizującym funkcje systemu informacyjnego wspierającego działanie usługi kluczowej;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

	• Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego KSC lub RODO;
Wysoki	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; • Ujawnienie zestawionej sesji zwrotnej z C&C, trwającej co najmniej od 30 minut, aktywnie wykorzystywanej przez atakującego (więcej niż 1kb/min); • Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w strefie chronionej; • Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; • Potwierdzona Informacja od osoby odpowiedzialnej za zaatakowany zasób informacyjny w zakresie administracji IT lub opieki nad usługą biznesową; • Informacja od Dyrektora lub Kierownika Departamentu Bezpieczeństwa; • Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; • Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; • Ujawnienie wycieku danych z chronionego obszaru z wykorzystaniem protokołów mailowych, upload na dyski webowe lub przenoszenie przez nieautoryzowane pendrive; • Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); • Ujawnienie nieznanego przez VirusTotal lub inne bazy reputacyjne oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu; • Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;
Średni	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie chronionym; • Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; • Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w środowisku chronionym;

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

	• Wszystkie przypadki wystąpienia na chronionych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy ale nie zostało zatrzymane przez inny system bezpieczeństwa; • Wszystkie potwierdzone przypadki z naruszenia poufności, dostępności lub integralności wykryte przez systemy bezpieczeństwa dla których użytkownik wyklucza świadome lub nieświadome działanie;
Niski	• Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu zdefiniowanego zdarzenia bezpieczeństwa opisanego scenariuszem reakcji, które udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

8. Transfer wiedzy

8.1. Zamawiający wymaga aby w każdym kwartale trwania umowy, Wykonawca przeprowadził dla grupy nie większej niż 8 osób wskazanych przez Koordynatora Zamawiającego warsztaty. Łączny wymiar godzin w kwartale wynosi nie więcej niż 24. Jedno spotkanie Warsztatowe trwa nie mniej niż 4 godziny i nie więcej niż 8 godzin.

8.2. Warsztaty swoim zakresem będę obejmować:

- Metody analizy i procedury monitorowania zdarzeń wykorzystywanych w ramach świadczonej usługi zgodnie z punktem 4
- Administracji Systemem opisanym w punkcie 5

8.3. Szczegółowy harmonogram warsztatów oraz lista uczestników zostaną uzgodnione przez Koordynatorów stron.

9. Raportowanie i rozliczanie pracy

9.1. Miesięczny Raport Rozliczenia Usług

9.1.1. Każdy miesiąc świadczenia Usług potwierdzony zostanie Protokołem Odbioru, wraz z Miesięcznym Raportem Rozliczenia Usług przygotowanym wg według wzoru uzgodnionego przez Koordynatorów w okresie przejściowym, o którym mowa w pkt 3.1. Wykonawca zobowiązany jest przedstawić Protokół Odbioru podpisany jednostronnie wraz z Miesięcznym Raportem Rozliczenia Usług w terminie 5 Dni Roboczych od dnia zakończenia miesiąca kalendarzowego, w którym była świadczona Usługa.

9.1.2. Zamawiający zastrzega sobie prawo zgłoszenia zastrzeżeń do Raportu, w terminie do 5 Dni roboczych od dnia jego otrzymania i zażądać uzupełnienia lub poprawy Raportu. Po uwzględnieniu przez Wykonawcę uwag do Protokołu Odbioru, w tym również Raportu Prac, Zamawiający w terminie kolejnych 3 Dni roboczych zweryfikuje ostateczną treść Protokołu Odbioru oraz Raportu Prac przed jego podpisaniem. W przypadku odmowy podpisania Raportu Prac przez Wykonawcę podstawę rozliczenia stanowi Raport Prac podpisany jednostronnie przez Zamawiającego.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

9.1.3. Podpisany przez Strony Protokół Odbioru wraz z Raportem Prac stanowi podstawę do rozliczenia wynagrodzenia za świadczenie Usługi w miesiącu, którego dotyczą i podstawę do ewentualnego naliczenia kar umownych za miesiąc, w którym nastąpiło przekroczenie parametrów SLA .

9.1.4. Poza pierwszym raportem, każdy kolejny obejmuje okres od godziny 0:00 pierwszego dnia miesiąca kalendarzowego do ostatniego dnia miesiąca kalendarzowego do godziny 23:59.

9.1.5. Raport praca składa się z sekcji:

9.1.5.1. Monitorowanie cyberbezpieczeństwa

- Data świadczenia usług
- Zestawienie poprawnie obsłużonych incydentów
  - Identyfikator incydentu
  - Nazwa
  - Klasyfikacja priorytetu Incydentu
  - Dokładna data i godzina ujawienia incydentu,
  - Dokładna data i godzina podjęcia incydentu
  - Dokładna data i godzina realizacji obsługi incydentu
  - Statusy końcowe
  - Liczba przygotowanych rekomendacji i raportów poincydentalnych
- Zestawienie niepoprawnie nieobsłużonych incydentów zgodnie z SLA
  - Identyfikator incydentu
  - Nazwa
  - Klasyfikacja priorytetu Incydentu
  - Dokładna data i godzina ujawnienia incydentu,
  - Dokładna data i godzina podjęcia incydentu
  - Dokładna data i godzina realizacji obsługi incydentu
  - Statusów końcowych zdarzenia (false-positive, zamknięty)
- Ogólne rekomendacje i zalecenia Zamawiającego w zakresie cyberbezpieczeństwa w nawiązaniu do obsłużonych Incydentów w celu eliminacji możliwości pojawienia się incydentów w przyszłości.

9.1.5.2. Utrzymanie Systemu SIEM

- Data świadczenia usług
- Zestawienie rekomendacji w zakresie zasobów Systemu SIEM
- Zestawienie wykorzystania licencji Systemu SIEM
- Zestawienie zbiorcze dla skonfigurowanych źródeł logów zawierające informacje
  - Liczba zgłoszonych przez Zamawiającego źródeł logów/systemów
  - Liczba poprawnie skonfigurowanych źródeł logów w systemie SIEM
  - Liczba źródeł logów poprawnie normalizowanych przez system SIEM
- Zestawienia wykonanych testów działania systemu wraz ze statusem wdrożonych działań w przypadku negatywnego wyniku testu.

9.1.5.3. Analiza złośliwego oprogramowania

- Data świadczenia usług

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

- Lista zgłoszonych analiz złośliwego oprogramowania
- Liczba analiz przeprowadzonych zgodnie z SLA

9.2. Dzienny Raport Rozliczenia Usług

9.2.1. Na żądanie Zamawiającego Wykonawca przedstawi Dzienny Raport Rozliczenia Usług za poprzedni dzień jednakże nie starszy niż 10 dni. Każdorazowo Dzienny Raport Rozliczenia Usług obejmuje okres od godziny 0:00 do godziny 23:59.

9.2.2. Raport składa się z sekcji:

- Za jaki okres jest zestawianie
- Zestawienie poprawnie obsłużonych incydentów:
  - Identyfikator incydentu
  - Nazwa
  - Klasyfikacja priorytetu Incydentu
  - Dokładna data i godzina ujawienia incydentu,
  - Dokładna data i godzina podjęcia incydentu
  - Dokładna data i godzina realizacji obsługi incydentu
  - Statusy końcowe
  - Ilość przygotowanych rekomendacji

9.3. Zamawiający przewiduje konieczność wysyłania raportów godzinowych zwierających informacje dotyczące liczby potwierdzonych Incydentów z podziałem na ich krytyczność od czasu wysłania ostatniego raportu.

10. Audyt

10.1. Wykonawca zobowiązuje się umożliwić Zamawiającemu lub wskazanemu przez niego podmiotowi przeprowadzanie audytów jakości prac Wykonawcy związanych z realizacją Umowy, w tym zgodności prowadzonych prac z postanowieniami Umowy. Wykonawca ma obowiązek zapewnić możliwość kontroli swoich prac, w szczególności niezwłocznie przekazać podmiotowi prowadzącemu audyt informacje i wyjaśnienia związane bezpośrednio z realizacją Umowy. Informacja o audycie i przedmiocie audytu zostanie przekazana Wykonawcy najpóźniej na 2 Dni Robocze przed terminem rozpoczęcia przeprowadzenia audytu. Z wykonania audytu Zamawiający sporządzi na piśmie protokół zaleceń poaudytowych i przekaże go Wykonawcy. Wykonawca zobowiązany jest do wprowadzenia na własny koszt i ryzyko zaleceń poaudytowych, wykazujących niezgodności w realizacji przez Wykonawcę Umowy. Wprowadzenie tych zaleceń poaudytowych nastąpi w terminie uzgodnionym przez Koordynatorów. W przypadku braku porozumienia co do terminu wprowadzenia ww. zaleceń poaudytowych obowiązuje termin wskazany przez Zamawiającego.

10.2. Zamawiający ma prawo do korzystania w związku z realizacją Umowy (w szczególności w związku z przeprowadzeniem kontroli realizacji Umowy, audytem, odbiorami lub jakimikolwiek innymi działaniami realizowanymi przez Zamawiającego) z usług upoważnionych przez niego podmiotów zewnętrznych. Zamawiający zobowiąże wskazane powyżej podmioty do zachowania poufności w odniesieniu do wszystkich informacji, w jakich posiadanie wejdą one w związku z prowadzonymi przez siebie czynnościami oraz do niewykorzystywania tych informacji w celu

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706

innym niż świadczenie prac na rzecz Zamawiającego. Wykonawca jest zobowiązany do współpracy z upoważnionymi podmiotami w pełnym zakresie wynikającym z upoważnienia, na zasadach określonych w Umowie względem Zamawiającego. W przypadku cofnięcia upoważnienia dla podmiotów zewnętrznych, Zamawiający jest zobowiązany do niezwłocznego poinformowania Wykonawcy o tym fakcie.

a) Wykonawca nie może odmówić wstępu do pomieszczeń, w których jest realizowana Umowa, udostępnienia żądanych informacji, dokumentów lub produktów związanych z realizacją Umowy, w tym mających wpływ na dochowanie terminów oraz zachowanie jakości, nawet jeśli objęte są tajemnicą przedsiębiorstwa. Zamawiający oraz osoby działające na jego rzecz zobowiązani są zachować informacje objęte tajemnicą przedsiębiorstwa Wykonawcy w poufności i mogą wykorzystać uzyskane w ten sposób informacje wyłącznie dla potrzeb kontroli, audytu, odbiorów lub innych działań realizowanych przez Zamawiającego.

b) Pozyskanie informacji niezbędnych do dokonania kontroli lub przeprowadzenia audytu nie może wiązać się dla Zamawiającego z dodatkowymi kosztami. W szczególności, na wniosek Zamawiającego Wykonawca zapewni obecność osób niezbędnych do zrealizowania zadań audytorskich w siedzibie Zamawiającego.

c) Wykonawca umożliwi Zamawiającemu przeprowadzenie do 2 audytów w ciągu 1 roku obowiązywania umowy.

11. Wymagania dodatkowe

11.1. Cała dokumentacja powinna być dostarczana w edytowalnej postaci elektronicznej, w formacie przetwarzanym przez MS Word, Excel lub PDF.

11.2. Zamawiający wymaga zatrudnienia przez Wykonawcę na podstawie umowy o pracę przez cały okres realizacji zamówienia 2 (dwóch) osób, wykonujących usługi w zakresie czynności Pierwszej Linii Wsparcia związanych z obsługą realizacji przedmiotu zamówienia, jeżeli wykonywane przez nich czynności polegają na wykonywaniu pracy w rozumieniu przepisu art. 22 § 1 ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (tj. Dz.U. 2023 poz.1465). Zamawiający uzna za spełniony obowiązek zatrudnienia osób wykonujących usługi w zakresie czynności pierwszej linii wsparcia przy realizacji przedmiotu zamówienia na podstawie umowy o pracę w przypadku, gdy Wykonawca skieruje do realizacji zamówienia własnych pracowników (dwóch) lub pracowników zatrudnionych na umowę o pracę. Zamawiający nie będzie ingerować w sposób prowadzenia działalności oraz organizację pracy administracyjno-biurowej Wykonawcy.

11.3. Wykonawca zobowiązany zostanie do przestrzegania polityki bezpieczeństwa opisanej w Polityce Bezpieczeństwa Informacji dla Wykonawców, która zostanie dołączona jako załącznik do umowy. O zmianach polityki mogących mieć wpływ na realizację umowy Wykonawca zostanie bezzwłocznie poinformowany.

Centrum e-Zdrowia
ul. Stanisława Dubois 5A
00-184 Warszawa
tel.: +48 22 597-09-27
fax: +48 22 597-09-37
biuro@cez.gov.pl | www.cez.gov.pl
NIP: 5251575309
REGON: 001377706