Załącznik nr 2 do Zapytania ofertowego

(Załącznik nr 1 do Projektowanych postanowień umownych)

Szczegółowy opis przedmiotu zamówienia

Przedmiotem zamówienia jest uruchomienie i utrzymanie zewnętrznej usługi SOC (Security Operations Center) wraz z niezbędnymi do realizacji usługi systemami teleinformatycznymi.

1. **Słownik pojęć:**

- **Cyberbezpieczeństwo –** odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.
- **Czas –** czas urzędowy obowiązujący w Polsce.
- **ZI** – Wydział Informatyki i Cyberbezpieczeństwa Urzędu Miasta Siemianowice Śląskie.
- **Dzień roboczy** – od poniedziałku do piątku z wyłączeniem dni ustawowo wolnych od pracy oraz dni wolnych u Zamawiającego.
- **Incydent** – zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo.
- **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.
- **Okres przejściowy** – czas, w którym Wykonawca zobowiązany będzie do podjęcia działań, których celem będzie przejęcie wiedzy od Zamawiającego o jego systemie monitoringu, uzgodnienia z Zamawiającym wzoru Miesięcznego Raportu Rozliczenia Usług, ustalenia z Zmawiającym harmonogramu wdrożenia dla pierwszych scenariuszy użycia oraz dopasowanie i uzgodnienie zasad współpracy Zamawiającego z systemami Wykonawcy. Zakończenie okresu przejściowego potwierdzone zostanie Protokołem Odbioru.
- **Koordynator Zamawiającego** – Naczelnik Wydziału Informatyki i Cyberbezpieczeństwa oraz Zastępca Naczelnika Wydziału Informatyki i Cyberbezpieczeństwa.
- **SOC** – Security Operations Center – centrum operacji bezpieczeństwa, którego zadaniem jest monitorowanie, zapobieganie, wykrywanie, badanie i reagowanie na cyberzagrożenia.
- **Praca ciągła** – praca systemu w trybie 24/7/365 dni.
- **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 dupa osobowymi.

- **KSC** – ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. 2024 poz. 1077 z późn. zm.)
- **Scenariusz Reakcji** – dokument opisujący wymagane czynności w przypadku wykrycia zdarzenia nieporządnego, składający się z:
    a) zestawu możliwości technicznych wykrycia zdarzenia;
    b) zdefiniowanych warunków wywołania zdarzenia niepożądanego;
    c) opisu identyfikacji zdarzeń zależnych;
    d) instrukcji reakcji na zdarzenie;
    e) instrukcji uruchomienia działań korekcyjnych;
    f) instrukcji wykonywania działań informacyjnych;
    g) 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:
    a) skonfigurowanie jednego lub kilku źródeł zdarzeń;
    b) 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 wymagana w zakresie jakościowym.
- **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.
- **System analizy logów** – system umożliwiający zbieranie i analizę logów z urządzeń, sieci i systemów informatycznych
- **Transfer Wiedzy** - usługa przekazywania kompetencji w zakresie realizacji usług Pierwszej i Drugiej Linii Wsparcia.
- **Usługa monitorowania Cyberbezpieczeństwa** – zestaw czynności wykonywanych przez Wykonawcę w ramach umowy w celu identyfikacji Incydentów.
- **Zdarzenia niepożądane** – zdarzenie mogące wskazywać na wystąpienie Incydentu w środowisku chronionym.
- **Zdarzenie False-Negative** – wykrycie przez Drugą 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.
- **Skuteczne powiadomienie** - przekazanie informacji i uzyskanie potwierdzenia jej przekazania. W szczególności skuteczne powiadomienie może zostać zrealizowane przez: rozmowę telefoniczną, wysłanie wiadomości i otrzymanie informacji o jej przeczytaniu w aplikacji mobilnej, wysłanie sms-a i otrzymanie odpowiedzi.

2. Termin realizacji usługi

1) Okresu przejściowy będzie trwał maksymalnie 2 miesiące.
2) Usługa SOC będzie realizowana od dnia zakończenia okresu przejściowego.
3) Uruchomienie usługi SOC wymaga zainstalowania, konfiguracji i przetestowania wszystkich źródeł logów, systemu analizy logów oraz systemu SIEM wraz z przygotowaniem Scenariuszy użycia systemu bezpieczeństwa oraz scenariuszy reakcji dla wszystkich monitorowanych systemów.
4) Wszystkie usługi będą realizowane przez okres 15 miesięcy od daty podpisania umowy.

3. Pierwsza i Druga Linia Wsparcia

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

1) Pierwsza Linia Wsparcia

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

   a) Monitorowanie zdarzeń naruszenia cyberbezpieczeństwa zgodnie warunkami określonymi w punkcie: Ogólne warunki SLA.
   b) Przeprowadzanie wstępnej oceny zdarzeń i realizowanie ustalonych Scenariuszy Reakcji.
   c) Analizę i eliminację najprostszych znanych zdarzeń określonych w ramach Scenariusza Reakcji.
   d) Łączenie (korelowanie) zdarzeń oraz incydentów cyberbezpieczeństwa.
   e) Dokumentowanie wykonanych czynności zgodnie z przygotowanymi i zaakceptowanymi Scenariuszami Reakcji.
   f) Eskalowanie zdarzenia zgodnie w ramach ustalonego Scenariusza Reakcji.
   g) Zamykanie zdarzeń błędnie rozpoznanych przez system bezpieczeństwa jako zagrożenie (tzw. False-Positive).
   h) Nadawanie priorytetu i kategoryzowanie zdarzeń bezpieczeństwa.
   i) Przygotowywanie miesięcznych raportów wykrytych zdarzeń bezpieczeństwa.

2) Druga Linia Wsparcia

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

   a) Dostępność usługi dla Zamawiającego zgodnie z określonymi warunkami SLA.
   b) Analizę zgłoszonych przez Pierwszą Linię Wsparcia Incydentów cyberbezpieczeństwa oraz przygotowanie raportów i zaleceń poincydentalnych.
   c) Przygotowywanie i realizację Scenariuszy użycia systemu bezpieczeństwa zgodnie z wymaganiami przedstawionymi przez Zamawiającego.
   d) Przygotowanie Scenariuszy Reakcji.
   e) Przygotowanie raportów incydentalnych oraz raportów na życzenie Zamawiającego.

f) nadzór nad poprawnością działania konfiguracji Scenariuszy użycia scenariuszy bezpieczeństwa.

4. Scenariusze

1) Scenariusz użycia systemu bezpieczeństwa

Zamawiający wymaga przygotowania i wdrożenia, przez Wykonawcę w okresie przejściowym nie mniej niż 100 możliwych Scenariuszy Reakcji dla zidentyfikowanych przez Wykonawcę ryzyk. Nowe Scenariusze oraz dedykowane dla Zamawiającego Scenariusze będą tworzone sukcesywnie podczas realizacji umowy. Minimalny zakres zadań, z których ma być zbudowany Scenariusz użycia systemu bezpieczeństwa zawiera:

- Skonfigurowanie jednego lub kilku źródeł zdarzeń.
- Stworzenie Scenariusza Reakcji w zakresie czynności wykonywanych przez Pierwszą Linię Wsparcia.
- Opisanie szczegółowej ścieżki eskalacji.

Wykonawca opracuje scenariusz sprawdzania poprawności działania. W przypadku pojawienia się nowych skuteczniejszych technik identyfikacji zagrożeń, Wykonawca ma obowiązek zaktualizować w porozumieniu z Zamawiającym istniejące Scenariusze użycia systemu bezpieczeństwa.

2) Scenariusz Reakcji

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

5. Priorytety Incydentów

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	Incydent spełnia definicję incydentu o priorytecie „Wysokim" oraz dodatkowo dotyczy zasobu mogącego przetwarzać lub przechowywać powyżej 50 rekordów danych objętych definicją rozporządzenia RODO. Zgłoszenie incydentu Poważnego skutkuje bezzwłocznym uruchomieniem u Zamawiającego procesu eskalacyjnego zgodnie z KSC lub RODO;
Wysoki	Incydent spełnia definicje incydentu o priorytecie „Średni" oraz dodatkowo spełnia co najmniej jedno z poniższych kryteriów: 1. Zestawienie zwrotnego kanału komunikacji z serwera dowodzenia i kontroli złośliwego oprogramowania trwającej co najmniej od 30 minut w tym aktywnie wykorzystywanego (więcej niż 1 kb/min); 2. Przełamanie zabezpieczeń aplikacji oraz ujawnienie nieznanych lub nieautoryzowanych procesów lub wątków aplikacyjnych lub systemowych w monitorowanych systemach; 3. Informacja od wiarygodnego sygnalisty w tym CSIRT NASK lub inny CSIRT stowarzyszony w ramach inicjatywy Trusted Introducers; 4. Potwierdzona informacja od pracownika ZI; 5. Zidentyfikowane oraz potwierdzone naruszenie integralności plików konfiguracyjnych, binariów lub skryptów aplikacji i/lub systemu operacyjnego; 6. Nieuprawniony dostęp i wykorzystanie uprawnień mogące pozwolić na utworzenie tylnej furtki, podsłuchu transmisji lub wykorzystania podatności; 7. Ujawnienie wycieku danych z monitorowanego systemu z wykorzystaniem protokołów sieciowych lub z wykorzystaniem nieautoryzowanych nośników przenośnych; 8. Ujawnienie nieautoryzowanego kodu służącego jako oprogramowanie administracyjne (tzw. adminware) lub ofensywnych technik przełamywania zabezpieczeń (tzw. grayware); 9. Ujawnienie nieznanego oprogramowania mającego złośliwe funkcje pozwalające operatorowi na uruchomienie nieautoryzowanych skryptów lub kodu; 10. Celowany atak na personel Zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w monitorowanym systemie; Zgłoszenie incydentu Wysokiego może spowodować uruchomienie u Zamawiającego procesu eskalacyjnego zgodnie z KSC lub RODO;

Priorytet	Opis
Średni	1. Zebrane dowody w systemach realizujących monitoring bezpieczeństwa świadczące o wystąpieniu co najmniej jednego wskaźnika na systemie monitorowanym; 2. Nieautoryzowane dysponowanie uprawnieniami administracyjnymi; 3. Częściowo personalizowany atak na personel zamawiającego z wykorzystaniem systemów komputerowych mający na celu wyłudzenie danych umożliwiających autoryzację w monitorowanyn systemie; 4. Wszystkie przypadki wystąpienia na monitorowanych systemach komputerowych złośliwego oprogramowania, które jest rozpoznawane przez system antywirusowy, ale nie zostało zatrzymane przez inny system bezpieczeństwa; **5.** 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, ale udało się potwierdzić, że wywołanie zdarzenia było efektem realizacji autoryzowanych czynności służbowych z pominięciem ustalonych procedur bezpieczeństwa.

6. Ogólne warunki SLA

Wykonawca zapewni świadczenie Usługi monitorowania zgodnie z określonym poziomem SLA.

Nazwa usługi	Poziom świadczonej usługi
Pierwsza Linia Wsparcia Czasy dla pierwszych zdarzeń każdego dnia w wymiarze 30 zdarzeń, pozostałe zadania realizowane będą w trybie ***„Best Effort”*** z wyłączeniem zdarzeń o priorytecie poważnym.	• Dostępność Pierwszej Linii Wsparcia w trybie 24/7/365. • Dostępność konsultanta w dni robocze pomiędzy godzinami 8:00 a 16:00.
Druga Linia Wsparcia Czasy dla pierwszych Incydentów każdego dnia w wymiarze 5 incydentów, pozostałe zadania realizowane w trybie ***„Best Effort”***	• Dostępność Drugiej Linii Wsparcia w dni robocze od godz. 8:00 do 16:00 • Dyżur telefoniczny Drugiej Linii Wsparcia w trybie 24/7/365 dla incydentów priorytecie Poważnym. • Dyżur telefoniczny Drugiej Linii Wsparcia, czekanie w gotowości na zgłoszenie z Pierwszej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Wysokim, w dni robocze od godz. 16:00 do godz. 8:00. • Dyżur telefoniczny Drugiej Linii Wsparcia, czekanie w gotowości na zgłoszenie z Pierwszej Linii Wsparcia, wyłącznie dla Incydentów o priorytecie Wysokim, w soboty, niedzielę i święta od godz. 8:00 do godz. 16:00.
Analiza złośliwego oprogramowania	Rozpoczęcie 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.

Scenariusz użycia systemu bezpieczeństwa	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.

1) 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 zobowiązany w ciągu 3 dni roboczych do przedstawienia pisemnego uzasadnienia odmowy, wskazując obiektywne czynniki świadczące o bezzasadności wniosku Wykonawcy.
2) Czas podjęcia Incydentu będzie liczony jako delta czasu pomiędzy odnotowaniem wystąpienia zdarzenia przez pierwsza linię wsparcia a czasem nadania priorytetu.
3) Czas realizacji Incydentu będzie liczony jako delta czasu pomiędzy podjęciem incydentu a zakończeniem obsługi podsumowanym wydanymi wstępnymi rekomendacjami i/lub raportem, w zależności od przypisanego scenariusza reakcji.
4) Wykonawca ma obowiązek skutecznego powiadomienia Koordynatora Zamawiającego o wystąpieniu:
   - Incydentu o priorytecie poważnym w czasie do 4 godzin od momentu odnotowania wystąpienia zdarzenia.
   - Incydentu o priorytecie wysokim w czasie do 8 godzin od momentu odnotowania wystąpienia zdarzenia.

7. Raport Poincydentalny

1) Zamawiający wymaga przygotowania wstępnego Raportu poincydentalnego umożliwiającego Wykonanie zgłoszenia zgodnie z wymaganiami KSC lub RODO w czasie do 24 godzin od momentu odnotowania incydentu o priorytecie poważnym.
2) Dla zdarzeń o priorytecie wysokim, dla których Zamawiający uruchomi proces eskalacji zgodnie z KSC lub RODO, Wykonawca przygotuje wstępny raport umożliwiający wykonanie zgłoszenia w czasie do 24 godzin od momentu otrzymania informacji o uruchomieniu procesu eskalacji od Zamawiającego.
3) Zamawiający wymaga przygotowania pełnego Raportu Poincydentalnego dla incydentów o priorytecie Poważnym i Wysokim nie później niż do 3 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) 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.

8. Wymagania minimalne dla Systemu Zbierania i Analizy Logów oraz Systemu SIEM.

W ramach realizacji usługi Wykonawca może użyć dowolnego systemu lub systemów spełniających łącznie opisane poniżej wymagania minimalne. Systemy zostaną zainstalowane na infrastrukturze Zamawiającego w formie maszyn wirtualnych systemu VMware. Zamawiający dostarczy system operacyjny Microsoft Windows Server 2022 Datacenter, jeśli będzie wymagany. Koszty udzielenia licencji, instalacji, konfiguracji, aktualizacji i utrzymania Systemu Zbierania i Analizy Logów oraz Systemu SIEM zostaną uwzględnione w kwocie miesięcznej za realizacje usługi SOC. Zamawiający nie przewiduje ponoszenia dodatkowych opłat w związku z korzystaniem z oprogramowania opisanego w niniejszym rozdziale.

Wykonawca do świadczenia usługi będzie wykorzystywał narzędzia dostarczone w niniejszym postępowaniu oraz udostępnione przez Zamawiającego. Dostęp do narzędzi i systemów Zamawiającego musi być zrealizowany za pomocą bezpiecznego połączenia szyfrowanego.

1) System Zbierania i Analizy Logów:
   - W ramach systemu logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące, gromadzące logi, korelujące zdarzenia i generujące raporty na podstawie danych z systemów bezpieczeństwa.
   - Rozwiązanie musi zostać dostarczone w postaci maszyn wirtualnej instalowanych w środowisku VMware.
   - Dane zbierane przez rozwiązanie powinny zawierać informacje co najmniej o: ruchu sieciowym, użytkownikach, aplikacjach i zagrożeniach.
   - Rozwiązanie musi umożliwiać obsługę incydentów na podstawie reguł wyszukujących automatycznie zdarzenia z logów.
   - Rozwiązanie musi mieć możliwość synchronizacji z serwerami czasu NTP.
   - Rozwiązanie musi mieć predefiniowane panele w postaci graficznej prezentacji zebranych informacji wykonane przez producenta.
   - Rozwiązanie musi umożliwiać gromadzenie zdarzeń za pomocą protokołów TCP oraz UDP.
   - Rozwiązanie musi umożliwiać bezpieczne gromadzenie danych przy pomocy protokołu TLS.

- Rozwiązanie musi umożliwiać przesyłanie logów do innego serwera logów (funkcja syslog forwarder).
- Rozwiązanie jest lokalne i wymaga instalacji w środowisku klienta.
- Rozwiązanie musi posiadać narzędzie dla łatwego przeszukiwania logów zebranych z podłączonych firewalli. Logi muszą być filtrowane na podstawie zapytań, które można stosować wielokrotnie.
- Rozwiązanie musi być wyposażone w wyszukiwanie zaawansowane w oparciu o wiele kryteriów (rodzaj logu, czas, itd.).
- Rozwiązanie musi być wyposażone w funkcjonalność wyświetlania rezultatów wyszukiwania co najmniej jako logi proste i graficzne.
- Rozwiązanie musi umożliwiać wykorzystanie zewnętrznych źródeł (CSV, IPtoHost, LDAP, GeoIP).
- Rozwiązanie musi umożliwiać nawigację na podstawie czasu (minut, godzin, dni, okresów)
- Rozwiązanie musi umożliwiać eksport wyników wyszukiwania w formacie CSV.
- Rozwiązanie musi umożliwiać tworzenie statycznych raportów.
- Musi istnieć możliwość zapisania stworzonych raportów do plików w formatach: PDF.
- Rozwiązanie musi umożliwiać zaplanowanie wykonania raportów.
- Rozwiązanie musi umożliwiać tworzenie własnych raportów.
- Rozwiązanie musi umożliwiać na podstawie kryteriów przeszukiwania logów utworzenie reguły alarmującej administratora. Reguła zostaje uaktywniona, gdy wszystkie kryteria zapytania zostaną spełnione. Powiadomienie musi mieć formę minimum wiadomości email.
- Rozwiązanie musi mieć funkcjonalność tworzenia incydentów z kryteriów zapytań i zarządzanie incydentami poprzez możliwość przypisywania osób do obsługi incydentów, komentowania incydentów, podejrzenia logów źródłowych które zawarte są w incydencie.
- System musi umożliwiać obsługę min 9000 zdarzeń na sekundę
- System musi umożliwiać przechowywanie, zarządzanie logami przez okres trwania usługi
- System musi umożliwiać obsługę wszystkich wymaganych urządzeń Zamawiającego

2) System SIEM:

- Wraz z systemem logowania i raportowania musi zostać dostarczone rozwiązanie monitorujące incydenty
- Rozwiązanie musi w pełni realizować swoją funkcjonalność lokalnie (instalacja on-prem)
- Architektura rozwiązania musi być oparta o fizyczne lub wirtualne sondy monitorujące, których rolą jest odbieranie kopii ruchu sieciowego, generowanie alarmów oraz/lub metadanych o zdarzeniach, przygotowanie przechwyconych plików do dalszej analizy oraz przekazywanie przetworzonych danych do urządzenia administracyjnego.
- Architektura rozwiązania musi być oparta także o urządzenie administrujące,

którego rolą jest zarządzanie sondami, włącznie z regułami detekcji, sygnaturami i nadzorem stanu, dogłębna analiza odebranych plików, prezentacja wyników detekcji, a także przekazywanie danych do rozwiązań stron trzecich

- Platformy muszą obsługiwać szyfrowanie dysków.
- Rozwiązanie musi wspierać implementację na środowisku wirtualnym takim jak VMware,
- Musi posiadać moduły zabezpieczone połączeniem (HTTPS) w przeglądarce
- Konsola rozwiązania musi zawierać informacje o kluczowych z punktu widzenia bezpieczeństwa detekcjach, uwzględniając adresy IP, adresy MAC, porty sieciowe, protokoły sieciowe, wyniki skanów plików, payload, sygnatury czasowe.
- Konsola rozwiązania musi szacować poziom ryzyka dla każdego wykrytego zagrożenia oraz musi dawać możliwość tagowania zdarzeń i załączania opisu (notatek).
- Rozwiązanie musi obsługiwać silniki detekcji takie jak Analiza Shellcode i Powershell, tj. detekcja technik wykorzystywanych przez cyberprzestępców w postaci specyficznego kodu służącego do wywoływania podatności oprogramowania zainstalowanego na stacjach roboczych czy serwerach.
- Rozwiązanie musi umożliwiać analizowanie całego ruchu sieciowego w oparciu o dostarczone reguły opisujące charakter niebezpiecznych połączeń.

3) Administracja Systemem Analizy Logów oraz Systemem SIEM

W ramach realizacji zadań administracji Systemem Analizy Logów oraz systemem SIEM Wykonawca będzie odpowiedzialny za:

a) Informowanie Zamawiającego o awariach, mogących uniemożliwić poprawne działanie systemów Zamawiającego i/lub świadczenie usług ujętych w niniejszym dokumencie.

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

c) Optymalizowanie konfiguracji.

d) Konfigurację Systemu Analizy Logów w celu gromadzenia i normalizowania logów ze wskazanych systemów Zamawiającego.

e) Weryfikację czy System Analizy Logów prawidłowo zapisuje oraz analizuje logi.

f) Tworzenie wymagań dla systemów Zamawiającego wysyłających logi w zakresie poziomu logowania zdarzeń.

4) Testowanie Systemu Analizy Logów oraz Systemu SIEM

W ramach realizacji zadań testowania Systemu Analizy Logów Wykonawca będzie odpowiedzialny za:

a) Przygotowanie i uzyskanie aprobaty Zamawiającego dla scenariuszy testów Systemu Analizy Logów.
b) Weryfikację prawidłowej konfiguracji źródeł logów.
c) Weryfikację wdrożonych scenariuszy użycia oraz implementacji nowych przypadków zgłoszonych przez Zamawiającego,
d) Weryfikację możliwości wdrożenia przypadków użycia w środowisku Zamawiającego,

9. Analiza złośliwego oprogramowania:

a) W ramach realizacji umowy, Zamawiający będzie mógł zlecić Wykonawcy wykonanie analizy złośliwego oprogramowania, nie więcej niż 3 w ciągu roku. Sposób zgłaszania analizy złośliwego oprogramowania zostanie uzgodniony po podpisaniu umowy.

b) 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,
- W przypadku wykorzystywania rodziny malware określenia wersji

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

10. Dodatkowe usługi w ramach SOC:

a) Wykonywanie testów podatności przy starcie usługi, a kolejne co 3 miesiące i przekazywanie Koordynatorowi Zamawiającego raportu z wykonanych testów.

b) Wykonanie testów penetracyjnych przy starcie usługi oraz po 12 miesiącach i przekazywanie Koordynatorowi Zamawiającego raportu z wykonanych testów.

c) Pomoc w wdrożeniu własnego rozwiązania skanera podatności.

11. Lista systemów Zamawiającego, wymagających monitoringu całodobowego i objętych usługą:

Lp.	Rodzaj usługi	Typ systemu operacyjnego	Czy dostępny z zewnątrz?	Krytyczny	Czy przetwarza dane osobowe
1.	Serwis www	Linux	Tak	Tak	Nie
2.	Serwer DNS	Linux	Tak	Tak	Nie
3..	Serwis www	Linux	Tak	Tak	Tak
4.	Baza danych Oracle	Linux	Nie	Tak	Tak
5.	Baza danych Postgres	Linux	Nie	Tak	Tak
6.	Microsoft Active Directory	Windows	Nie	Tak	Tak
7.	Serwer plików	Windows	Nie	Tak	Tak
8.	Serwer plików	Windows	Nie	Tak	Tak
9.	Usługa RDP	Windows	Tak	Nie	Nie
10.	Serwis www	Linux	Tak	Nie	Nie
11.	Serwis www	Linux	Tak	Tak	Tak
12.	Poczta elektroniczna	Linux	Tak	Tak	Tak
13.	Poczta elektroniczna	Linux	Tak	Tak	Tak
14.	Klaster UTM Active/Passive z pakietem zabezpieczeń		Nie	Tak	Nie
15.	Routing sieci wewnętrznych (CISCO z Data Flow)	CISCO	Nie	TAK	Nie