Załącznik nr 1 do Zapytania Ofertowego

Opis Przedmiotu Zamówienia

Wdrożenie SZBI, usługi SOC oraz szkolenia dla personelu

Katowice, grudzień 2025

# Informacje wstępne

Zamówienie niniejsze jest prowadzone w ramach projektu „Rozwój usług cyfrowych i poprawa cyberbezpieczeństwa w Szpitalu Zakonu Bonifratrów pw. Aniołów Stróżów w Katowicach. Nr wniosku KPOD.07.03-IP.10-0131/25” finansowanego ze środków Krajowego Planu Odbudowy i Zwiększania Odporności, Priorytet Efektywność, dostępność i jakość systemu ochrony zdrowia - część grantowa, Działanie D1.1.2. Przyspieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia, nr naboru: KPOD.07.03-IP.10-001/25.

Celem zamówienia jest podniesienie poziomu cyberbezpieczeństwa Zamawiającego poprzez inwestycję w zintegrowany system ochrony, zarządzania i edukacji.

# Wymagania ogólne dla urządzeń i oprogramowania sieciowego.

## Model Płatności i Gwarancja Ciągłości

1. **Charakter Inwestycyjny:** Zamówienie realizowane jest w modelu zakupu inwestycyjnego (jednorazowego). Wszystkie elementy zamówienia, w tym licencje i usługi wsparcia (SOC, Security Officer, Platforma E-learning), traktowane są jako jednolity wydatek inwestycyjny.
2. **Płatność z góry:** Zamawiający nie dopuszcza modelu płatności abonamentowych (miesięcznych). Wykonawca zobowiązany jest wycenić dostawę pakietów usług i licencji opłaconych z góry na pełny okres 36 miesięcy.
3. **Gwarancja Ciągłości Działania:** Z uwagi na jednorazowy charakter płatności, Wykonawca udziela **nieodwołalnej, 36-miesięcznej gwarancji ciągłości świadczenia usług**. Gwarancja ta obejmuje:
   * Utrzymanie aktywności licencji i subskrypcji EDR.
   * Zapewnienie ciągłości monitorowania SOC w trybie 24/7/365.
   * Dostępność platformy e-learningowej.
   * Świadczenie nadzoru autorskiego nad SZBI. W przypadku utraty ciągłości usług z przyczyn leżących po stronie Wykonawcy, Wykonawca zobowiązany będzie do zwrotu wynagrodzenia proporcjonalnie do niewykorzystanego okresu, niezależnie od innych kar umownych.

## Legalność i Kanał Dystrybucji

Całość oprogramowania i sprzętu musi pochodzić z autoryzowanego kanału sprzedaży producentów na rynek Unii Europejskiej. Wykonawca dostarczy certyfikaty licencyjne potwierdzające opłacenie wsparcia i subskrypcji na wymagany okres.

## Dostępność Cyfrowa (KPO)

Mając na uwadze, że zamówienie jest finansowane ze środków publicznych, Zamawiający podlega przepisom Ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych (Dz.U. 2023 poz. 1440). Wykonawca zobowiązany jest zapewnić, aby wszystkie dostarczone produkty cyfrowe (w szczególności platforma e-learningowa, interfejsy raportowe SOC udostępniane Zamawiającemu oraz materiały szkoleniowe) spełniały wymagania **WCAG 2.1 na poziomie co najmniej AA**.

## Zasada DNSH (Do No Significant Harm)

W zakresie, w jakim realizacja zamówienia wiąże się z wykorzystaniem centrów przetwarzania danych (usługi chmurowe SOC, EDR, E-learning), Wykonawca gwarantuje, że infrastruktura ta spełnia wymogi efektywności energetycznej zgodnie z "Code of Conduct for Energy Efficiency in Data Centres" lub normą równoważną, co jest warunkiem kwalifikowalności wydatku w ramach KPO (inwestycja D.1.1.2).

# Zakres zamówienia

## Zakres zamówienia podstawowego (Gwarantowany)

Zakres niniejszego zamówienia obejmuje Szpital Zakonu Bonifratrów pw. Aniołów Stróżów w Katowicach i dotyczy następujących pakietów:

|  |  |  |  |
| --- | --- | --- | --- |
| **Nazwa pozycji** | **Ilość** | **J.m.** | **Opis i charakterystyka zakupu (Inwestycja)** |
| **Pakiet SOC (36 m-cy)** | 1 | kpl. | Zakup i wdrożenie zintegrowanej usługi monitorowania (Sonda/SIEM) wraz z opłaconym z góry pakietem obsługi analitycznej i operatorskiej na okres 36 miesięcy. |
| **Pakiet EDR (36 m-cy)** | 1 | kpl. | Dostawa terminowych licencji oprogramowania EDR dla 35 serwerów i 300 stacji roboczych, opłaconych z góry na okres 36 miesięcy. |
| **Wdrożenie SZBI** | 1 | szt. | Usługa jednorazowa polegająca na opracowaniu i wdrożeniu dokumentacji oraz procesów (Security Officer – faza wdrożeniowa). |
| **Pakiet Security Officer (36 m-cy)** | 1 | kpl. | Zakup pakietu nadzoru autorskiego nad SZBI (utrzymanie, aktualizacje, szkolenia) na okres 36 miesięcy (płatne jednorazowo). |
| **Szkolenie kadry kierowniczej** | 1 | szt. | Przeprowadzenie warsztatu stacjonarnego dla kadry zarządzającej (do 27 osób). |
| **Pakiet szkoleniowy E-learning** | 1 | kpl. | Uruchomienie platformy i zapewnienie dostępu do szkoleń dla personelu (600 użytkowników) na okres 36 miesięcy (płatne jednorazowo). |

## Prawo Opcji (Streszczenie)

Zamawiający przewiduje możliwość rozszerzenia zamówienia o jednostki powiązane (szczegóły w Rozdziale "Prawo Opcji"):

1. **Element 1:** Pakiety SOC i EDR dla oddziałów (Kraków, Warszawa, Wrocław, Łódź, Centrala).
2. **Element 2:** Dodatkowe szkolenia stacjonarne dla kadry w oddziałach.
3. **Element 3:** Rozszerzenie platformy e-learningowej o dodatkowych użytkowników.
4. **Element 4:** Wdrożenie SZBI w oddziałach.
5. **Element 5:** Pakiet Security Officer dla oddziałów.

# Szczegółowy opis przedmiotu zamówienia

## SOC

|  |
| --- |
| Przedmiotem zamówienia jest dostawa, wdrożenie i utrzymanie **rozwiązania SOC w postaci zintegrowanej Sondy bezpieczeństwa**. Rozwiązanie ma zapewnić całodobowe monitorowanie, analizę, wykrywanie oraz zarządzanie ryzykiem cybernetycznym w infrastrukturze Zamawiającego, obejmującej środowiska IT, OT oraz IIoT. System ma łączyć funkcjonalności techniczne z działaniami organizacyjnymi, tworząc spójny ekosystem ochrony cybernetycznej, zgodny z regulacjami prawnymi oraz najlepszymi praktykami branżowymi (w tym standardami ISO/IEC 27001, ISO/IEC 22301, Dyrektywę Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (NIS2), Ustawę z dnia 25 czerwca 2025 r. o krajowym systemie certyfikacji cyberbezpieczeństwa (Dz.U. 2025 poz. 1017)).  **System należy dostarczyć wraz z opłaconym z góry Pakietem Utrzymaniowym na okres 36 miesięcy. Pakiet ten musi gwarantować ciągłość działania rozwiązania, aktualizacje sygnatur oraz dostępność obsługi analitycznej (SOC) w trybie 24/7/365 bez konieczności ponoszenia przez Zamawiającego dodatkowych opłat licencyjnych lub abonamentowych w trakcie trwania okresu trwałości.**   1. **Cele i ogólne wymagania**   Wdrożona usługa powinna umożliwiać: stałe monitorowanie systemów i urządzeń, natychmiastowe wykrywanie oraz obsługę incydentów bezpieczeństwa, gromadzenie, analizę i korelację danych o zagrożeniach, zarządzanie podatnościami i rekomendowanie działań naprawczych, prowadzenie analiz informatyki śledczej (forensic) oraz raportowanie do organów nadzoru, wsparcie operacyjne, taktyczne i strategiczne w zakresie bezpieczeństwa informacji oraz bezpieczeństwa teleinformatycznego, szkolenie i podnoszenie świadomości pracowników.  Zamawiający wymaga zaoferowania usługi na okres 36 miesięcy.   1. **Zakres funkcjonalny i zadania wykonawcy**   3.1 Monitorowanie i zarządzanie zdarzeniami  Zadania wykonawcy: uruchomienie monitoringu sieci, systemów, aplikacji, urządzeń OT/IIoT w trybie 24/7/365. Konfiguracja systemu do rejestrowania i klasyfikacji wszystkich zdarzeń bezpieczeństwa. Opracowanie mechanizmów wczesnego wykrywania anomalii i incydentów. Przygotowanie i dostarczanie Zamawiającemu okresowych raportów bezpieczeństwa. Wdrożenie systemu do zarządzania podatnościami, wraz z harmonogramem regularnych skanowań podatności. Automatyzacja czynności hardeningu systemów teleinformatycznych i sieci (usuwanie zbędnych usług, aktualizacje, poprawa konfiguracji).   1. Operator usługi zobowiązany jest do zapewnienia ciągłości procesu detekcji oraz reakcji na incydenty bezpieczeństwa teleinformatycznego. Zakres obowiązków obejmuje w szczególności: bieżące monitorowanie systemów i komponentów infrastruktury, przyjmowanie i rejestrowanie zgłoszeń dotyczących potencjalnych zdarzeń, realizację procesu triage w celu klasyfikacji i priorytetyzacji incydentów, analizę zdarzeń i incydentów bezpieczeństwa oraz udzielanie wsparcia w zakresie działań mitygacyjnych. Realizacja powyższych zadań winna być zgodna z uznanymi standardami zarządzania incydentami bezpieczeństwa (m.in. ISO/IEC 27035, NIST SP 800-61). 2. Operator usługi zobowiązany jest do każdorazowego sporządzenia raportu dotyczącego zdarzenia bądź incydentu bezpieczeństwa teleinformatycznego. Raport winien obligatoryjnie zawierać co najmniej: określenie poziomu krytyczności/powagi incydentu, charakterystykę zdarzenia wraz z jego podstawowymi atrybutami identyfikacyjnymi, szczegółowy opis działań podjętych przez Operatora, udokumentowanie działań wykonanych po stronie Zamawiającego, a także wszelkie inne informacje niezbędne do prawidłowej klasyfikacji, obsługi oraz zamknięcia incydentu zgodnie z obowiązującymi procedurami bezpieczeństwa. Raport powinien być zgodny ze standardem Traffic Light Protocol (TLP). Operator usługi powinien zarządzać statusem zdarzenia lub incydentu bezpieczeństwa w systemie SIEM Zamawiającego, dokumentować jego przebieg oraz raportować ewentualne problemy z realizacją remediacji incydentu. 3. Operator usługi zobowiązany jest do zapewnienia mechanizmów umożliwiających przyjęcie informacji o zdarzeniu lub incydencie bezpieczeństwa teleinformatycznego z wykorzystaniem zewnętrznych kanałów komunikacyjnych. Minimalny zestaw wymaganych kanałów obejmuje: dedykowaną infolinię telefoniczną, skrzynkę poczty elektronicznej (e-mail) oraz system zgłoszeniowy klasy Service Desk/Incident Management. Wszystkie wymienione kanały winny gwarantować integralność, dostępność i poufność przekazywanych danych oraz umożliwiać rejestrowanie zgłoszeń zgodnie z wymaganiami norm ISO/IEC 27035 oraz ISO/IEC 20000.Operator usługi zobowiązany jest do zapewnienia nieprzerwanej (24/7/365) gotowości do realizacji procesu eskalacji incydentów bezpieczeństwa teleinformatycznego zgodnie z uprzednio uzgodnioną i zatwierdzoną procedurą eskalacyjną. Procedura ta winna gwarantować ścisłe odwzorowanie ścieżek decyzyjnych oraz poziomów odpowiedzialności, zapewniając terminowe zaangażowanie odpowiednich interesariuszy. W ramach eskalacji Operator usługi musi zapewnić dedykowany potencjał ludzki odpowiedzialny za koordynację działań remediacyjnych, bieżącą komunikację z Zamawiającym oraz formułowanie rekomendacji dotyczących dalszych kroków technicznych i organizacyjnych, niezbędnych do skutecznego ograniczenia skutków incydentu oraz zapobieżenia jego eskalacji. 4. Operator usługi zobowiązany jest do przeprowadzenia klasyfikacji każdej informacji, której pozostaje właścicielem, w zakresie identyfikacji oraz przypisania odpowiedniej grupy odbiorców uprawnionych do uzyskania dostępu do treści o charakterze wrażliwym. Operator zapewnia, iż każda jednostka informacji zostanie uzupełniona o stosowną klasyfikację przed jej dalszym wykorzystaniem w realizowanych procesach bezpieczeństwa, zgodnie z wymaganiami norm ISO/IEC 27001 oraz ISO/IEC 27005. 5. Operator usługi jest zobowiązany do identyfikowania, katalogowania i utrzymywania rejestru informacji dotyczących zasobów teleinformatycznych Zamawiającego, obejmującego co najmniej: właścicieli poszczególnych zasobów, ich lokalizację oraz krytyczność/wagę dla procesów biznesowych. Wymagane jest wdrożenie mechanizmów umożliwiających bieżące zarządzanie cyklem życia tych informacji, z uwzględnieniem integralności i spójności danych. 6. Operator usługi zobowiązany jest do iteracyjnej analizy dostępnych danych telemetrycznych i kontekstowych w celu wykrywania, izolowania i eskalowania zaawansowanych zagrożeń, które mogą pozostawać niewidoczne dla systemu klasy SIEM eksploatowanego przez Zamawiającego. Analizy te muszą obejmować zarówno anomalie behawioralne, jak i złożone wskaźniki kompromitacji (IOC/IOA). 7. Operator usługi zobowiązany jest do prowadzenia analizy próbek oprogramowania potencjalnie złośliwego w trybie 24/7/365, obejmującej określenie wektora infekcji, technik egzekucji kodu, wpływu na środowisko teleinformatyczne, a także identyfikację skutków wtórnych (persistent mechanisms, lateral movement, data exfiltration). Wyniki analizy muszą być dostarczane w formie ekspertyz technicznych, zawierających zarówno aspekty taktyczne, jak i strategiczne. 8. Operator usługi winien dysponować komercyjnym, utrzymywanym w aktualnej wersji narzędziem klasy sandbox/dynamic malware analysis, umożliwiającym detekcję ataków typu zero-day, monitorowanie aktywności plików, procesów, pamięci oraz sieci, a także identyfikację wskaźników kompromitacji (IOC). 9. Operator usługi zobowiązany jest do świadczenia usług konsultingowych na rzecz Zamawiającego, zapewniając dostęp do kompetencji specjalistów w zakresie cyberbezpieczeństwa, w szczególności w obszarach analizy technicznej incydentów, rekomendacji działań naprawczych oraz wsparcia przy wdrożeniu mechanizmów podwyższających dojrzałość procesów bezpieczeństwa. Operator winien zagwarantować dostępność wymaganych zasobów ludzkich w trybie uzgodnionym z Zamawiającym. 10. Operator usługi jest zobligowany do spełnienia wymagań 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 (Dz.U. 2019 poz. 2479). Operator zobowiązany jest do utrzymywania zgodności operacyjnej i proceduralnej z powyższym aktem prawnym przez cały okres obowiązywania umowy. 11. Operator usługi powinien posiadać wdrożony i certyfikowany przez akredytowaną jednostkę certyfikującą System Zarządzania Bezpieczeństwem Informacji spełniający wymagania standardu ISO 27001 w zakresie cyberbezpieczeństwa. 12. Operator usługi zobowiązany jest do cyklicznego raportowania statusu nierozwiązanych incydentów oraz zdarzeń bezpieczeństwa teleinformatycznego. Raportowanie winno być realizowane w odstępach nie dłuższych niż 24 godziny i obejmować przekazanie Zamawiającemu aktualnych informacji dotyczących charakteru incydentu/zdarzenia, jego statusu, zidentyfikowanych ryzyk oraz dotychczas podjętych działań naprawczych i planowanych kolejnych kroków. Forma raportu powinna umożliwiać jednoznaczną identyfikację incydentu oraz śledzenie jego obsługi w czasie rzeczywistym, zgodnie z obowiązującą procedurą zarządzania incydentami (ISO/IEC 27035, NIST SP 800-61). Operator usługi zobowiązany jest do zapewnienia kompleksowej obsługi zdarzeń oraz incydentów bezpieczeństwa teleinformatycznego w pełnej zgodności z wewnętrznymi politykami bezpieczeństwa informacji, procedurami operacyjnymi oraz regulacjami organizacyjnymi obowiązującymi u Zamawiającego. Obsługa ta winna obejmować wszystkie etapy procesu zarządzania incydentem, począwszy od detekcji, rejestracji i klasyfikacji, poprzez analizę i eskalację, aż po działania remediacyjne, zamknięcie i raportowanie. Operator ma obowiązek każdorazowo dostosować metodykę działania do obowiązujących u Zamawiającego standardów, zapewniając spójność z ramami prawnymi, regulacyjnymi i normatywnymi (m.in. ISO/IEC 27001, ISO/IEC 27035, NIS2). 13. Operator usługi powinien posiadać zdolność do realizacji testów bezpieczeństwa systemów teleinformatycznych, weryfikacji bezpieczeństwa oprogramowania wykonywalnego dla systemów Microsoft Windows, Linux, OSX oraz Android a także analiz architektury bezpieczeństwa. 14. Operator usługi powinien posiadać zdolność do weryfikacji artefaktów takich jak adres IP, hash pliku, adres e-mail, domena w zewnętrznych źródłach threat intelligence oraz w historii incydentów Zamawiającego. 15. Operator usługi zobowiązany jest do sprawowania nadzoru nad ewolucją oraz rozwojem utrzymywanego modelu bezpieczeństwa teleinformatycznego Zamawiającego. W szczególności Operator winien dostarczać rekomendacje strategiczne i taktyczne adresowane do poziomu zarządczego, oparte na systematycznej analizie ryzyk identyfikowanych w ramach świadczonych procesów bezpieczeństwa. Rekomendacje te muszą obejmować zarówno aspekty technologiczne, organizacyjne, jak i proceduralne, z uwzględnieniem bieżących trendów zagrożeń, luk w istniejących mechanizmach kontrolnych oraz zgodności z obowiązującymi regulacjami i standardami (m.in. ISO/IEC 27001, ISO/IEC 27005, NIST CSF). Operator odpowiada za zapewnienie, iż przekazywane rekomendacje będą stanowiły podstawę dla decyzji strategicznych w obszarze zarządzania ryzykiem oraz podnoszenia dojrzałości modelu bezpieczeństwa. 16. Operator usługi zobowiązany jest do opracowywania cyklicznych rekomendacji dotyczących rozwoju i doskonalenia modelu bezpieczeństwa teleinformatycznego Zamawiającego. Rekomendacje te muszą być oparte na analizie informacji oraz ryzyk zidentyfikowanych w toku obsługi incydentów bezpieczeństwa, przy czym powinny wskazywać zarówno nieprawidłowości i luki kontrolne, jak i możliwe usprawnienia techniczne, organizacyjne i proceduralne. Operator odpowiada za dostarczenie rekomendacji w sposób sformalizowany, umożliwiający ich wykorzystanie przez Zamawiającego do podejmowania decyzji zarządczych w obszarze bezpieczeństwa informacji. 17. Operator usługi zobowiązany jest do zapewnienia wsparcia merytorycznego w zakresie interpretacji i stosowania obowiązujących wymagań prawnych odnoszących się do bezpieczeństwa teleinformatycznego, ochrony danych osobowych (w tym RODO/GDPR), świadczenia usług kluczowych (zgodnie z ustawą o KSC oraz dyrektywą NIS2), świadczenia usług cyfrowych (m.in. eIDAS) oraz innych aktów legislacyjnych właściwych dla działalności Zamawiającego. Wsparcie to obejmuje zarówno bieżącą interpretację przepisów, jak i formułowanie rekomendacji dostosowawczych, zapewniających zgodność operacyjną i regulacyjną w obszarze cyberbezpieczeństwa.   3.2. Reakcja na incydenty  Proces reakcji na incydenty bezpieczeństwa realizowany zwłaszcza poprzez:   1. opracowanie i wdrożenie procedur reagowania na incydenty - przygotowanie i implementacja procedur zgodnych z wymaganiami dyrektywy NIS2, ustawy o krajowym systemie cyberbezpieczeństwa (KSC) oraz powiązanych aktów wykonawczych, uwzględniających pełny cykl życia incydentu (detekcja, analiza, eskalacja, remediacja, zamknięcie); proces powinien zostać zamodelowany w standardzie BPMN 2.0; 2. organizacja sztabów kryzysowych - zaprojektowanie i wdrożenie zasad funkcjonowania sztabów kryzysowych, w tym schematów decyzyjnych, ścieżek eskalacyjnych, podziału ról i odpowiedzialności oraz mechanizmów komunikacji wewnętrznej i zewnętrznej; 3. zapewnienie udziału ekspertów - zagwarantowanie udziału ekspertów z obszarów: cyberbezpieczeństwa, ochrony danych osobowych (RODO/GDPR) oraz zgodności prawnej, celem zapewnienia wieloaspektowego wsparcia w obsłudze incydentów oraz zgodności działań z obowiązującymi regulacjami; 4. wsparcie techniczne w zakresie przywracania systemów - udział w działaniach przywracających pełną funkcjonalność systemów i usług teleinformatycznych, w tym w szczególności w zakresie analizy przyczyn źródłowych (root cause analysis), działań naprawczych oraz odbudowy środowisk produkcyjnych; 5. sporządzanie raportów - przygotowywanie raportów powłamaniowych (post-incident / post-mortem reports) wymaganych przez regulatorów i właściwe organy nadzorcze, w tym CSIRT sektorowy/krajowy oraz Urząd Ochrony Danych Osobowych (UODO), zgodnie z terminami i zakresem określonym w obowiązujących przepisach; 6. opracowanie wniosków i działań korygujących - formułowanie rekomendacji oraz planów działań korygujących po zakończeniu obsługi incydentu, w celu minimalizacji ryzyka wystąpienia podobnych zdarzeń w przyszłości, wraz z propozycjami usprawnień organizacyjnych, technicznych i proceduralnych.   3.3. SIEM (Security Information and Event Management)  Wykonawca w ramach implementacji systemu SIEM zapewni:   1. instalację i konfigurację systemu SIEM - wdrożenie rozwiązania obejmującego wybrane komponenty środowiska teleinformatycznego Zamawiającego, w tym infrastrukturę IT, systemy OT (Operational Technology) oraz komponenty IIoT (Industrial Internet of Things), z uwzględnieniem specyfiki heterogenicznych protokołów komunikacyjnych oraz wymagań w zakresie wysokiej dostępności; 2. centralizację logów i zdarzeń - implementację mechanizmów agregacji i bezpiecznego przechowywania logów oraz zdarzeń w scentralizowanym repozytorium, zapewniającym integralność, poufność i nienaruszalność danych oraz spełniającym wymogi regulacyjne (m.in. KSC, NIS2, ISO/IEC 27001); 3. implementację reguł korelacji - konfigurację reguł i mechanizmów analitycznych umożliwiających identyfikację wzorców ataków, anomalii behawioralnych i nieautoryzowanych aktywności, z odwołaniem do uznanych ram referencyjnych (np. MITRE ATT&CK, ENISA Threat Landscape); 4. integrację z systemami zarządzania bezpieczeństwem - zapewnienie dwukierunkowej integracji SIEM z istniejącymi systemami bezpieczeństwa Zamawiającego (m.in. SOAR, IAM, EDR/XDR, NDR), w celu umożliwienia spójnej orkiestracji i automatyzacji procesów detekcji oraz reakcji; 5. automatyczne generowanie alertów i powiadomień – konfigurację mechanizmów tworzenia alertów bezpieczeństwa oraz ich przekazywania do zespołu SOC w trybie 24/7/365, z uwzględnieniem priorytetyzacji incydentów oraz minimalizacji liczby fałszywych pozytywów (false positives).   3.4. SOAR (Security Orchestration, Automation and Response)  Wykonawca w ramach implementacji systemu SOAR zapewni:   1. wdrożenie platformy SOAR - instalację niezbędnych komponentów, integrację komponentów w platformą SOAR, konfigurację w celu zapewnienia spójnej orkiestracji procesów detekcji, analizy i reakcji na incydenty; 2. opracowanie i implementacja playbooków - stworzenie zestawu playbooków automatyzujących obsługę najczęściej występujących scenariuszy incydentów, np. ataki typu ransomware, phishing, infekcje złośliwym oprogramowaniem (malware), próby nieautoryzowanego dostępu czy nadużycia kont użytkowników. Playbooki muszą być zgodne z uznanymi standardami (np. NIST SP 800-61, MITRE ATT&CK) oraz dostosowane do specyfiki środowiska Zamawiającego; 3. konfiguracja procesów automatycznej reakcji - implementacja procedur umożliwiających automatyzację reakcji na incydenty, w tym np.: izolację stacji roboczej/serwera, blokowanie adresów IP i domen, reset haseł lub blokadę kont użytkowników, aktualizację reguł w systemach zabezpieczeń. Automatyzacja musi uwzględniać mechanizmy walidacji i autoryzacji działań krytycznych zgodnie z politykami bezpieczeństwa Zamawiającego. 4. dokumentowanie i raportowanie działań - zapewnienie pełnej rejestracji (audit trail) wszystkich czynności wykonywanych przez platformę SOAR oraz przygotowywanie raportów operacyjnych i zarządczych dotyczących efektywności automatyzacji, skuteczności reakcji oraz zgodności z politykami bezpieczeństwa. Raporty powinny być dostarczane w formie cyklicznej oraz na żądanie Zamawiającego.   3.5. Zarządzanie podatnościami i testami penetracyjnymi  Wykonawca w ramach implementacji systemu SOAR procesu zarządzania podatnościami i testami penetracyjnymi zapewni:   1. Opracowanie harmonogramu cyklicznych skanów podatności (co najmniej raz na kwartał) w dostarczonym narzędziu. 2. Integracje z wybranymi skanerami podatności (np., Nessus, OpenVAS). 3. Wykonanie skanów podatności zgodnie z harmonogramem z wykorzystaniem dostarczonego narzędzia. 4. Opracowanie raportu w dostarczonym narzędziu, 5. Omówienie rekomendacji wynikających z przeprowadzonego skanowania z Zamawiającym. 6. Porównanie wyników skanowania z wcześniejszymi skanami w dostarczonym narzędziu.   3.6. Threat Intelligence  Wykonawca w ramach implementacji procesu Threat Intelligence zapewni:   1. Integracja z komercyjnymi i otwartymi źródłami Threat Intelligence. 2. Analiza i agregacja danych o aktualnych kampaniach cyberataków. 3. Wdrożenie systemu wczesnego ostrzegania o nowych podatnościach i malware. 4. Integracje TI z SIEM w celu korelacji danych i przyspieszenia reakcji SOC.   3.7. Forensic / Analiza śledcza  Wykonawca w ramach implementacji procesu Forensic zapewni:   1. Wdrożenie procedur zabezpieczania dowodów cyfrowych zgodnych z wymogami prawnymi. 2. Analizę ścieżki ataku, sposobów kompromitacji i użytych narzędzi. 3. Przygotowanie raportów z analizy śledczej dla Zarządu oraz organów regulacyjnych. 4. Wsparcie przy audytach zgodności.   3.8. Honeypot / Deception  Wykonawca w ramach implementacji Honeypot zapewni:   1. Zaprojektowanie i wdrożenie systemu honeypot w środowisku Zamawiającego. 2. Rejestracja prób włamania i analiza metod intruzów. 3. Generowanie raportów o nowych zagrożeniach wykrytych w środowisku testowym. 4. Dostarczanie wczesnych ostrzeżeń o aktywnych atakach.   **4. Integracja funkcjonalności**  Zintegrowana Sonda bezpieczeństwa ma działać jako spójny ekosystem, w którym:   * SIEM agreguje dane i przekazuje je do SOC, * SOC analizuje zdarzenia i inicjuje działania, * SOAR automatyzuje odpowiedzi na powtarzające się incydenty, * Threat Intelligence dostarcza aktualnych informacji o zagrożeniach, * Forensic umożliwia pełną analizę incydentów, * Honeypot dostarcza danych o nowych technikach ataków, * Pełnomocnik ds. bezpieczeństwa koordynuje wszystkie działania zapewniając zgodność z regulacjami.   **5. Wymagania formalne**  5.1. Service Level Agreement (SLA)   * + Dostawca zapewni dostępność usługi monitoringu na poziomie min. 99,5% w skali miesiąca.   + Reakcja na incydenty krytyczne – do 30 minut.   + Reakcja na incydenty wysokiego priorytetu – do 2 godzin.   + Reakcja na incydenty średniego priorytetu – do 24 godzin.   + Reakcja na incydenty niskiego priorytetu – do 72 godzin.   Niedotrzymanie parametrów SLA (np. czasu reakcji) skutkować będzie naliczeniem kar umownych zgodnie z zapisami Umowy. Z uwagi na jednorazowy charakter płatności za Pakiet SOC, Wykonawca zobowiązany jest do zapłaty kar na wezwanie Zamawiającego. Raporty miesięczne z poziomu świadczenia usług (SLA) będą stanowiły podstawę do weryfikacji jakości, a nie podstawę do wystawienia faktury.  5.2. Raportowanie   * + Raporty miesięczne: szczegółowa analiza incydentów, podatności, zrealizowanych działań.   + Raporty kwartalne: zestawienie trendów i rekomendacje strategiczne.   + Raporty roczne: podsumowanie działań, analiza ryzyka, rekomendacje na kolejny okres.   + Raporty miesięczne stanowią dowód realizacji zobowiązania Gwarancji Ciągłości Usług. Brak dostarczenia raportu lub wykazanie w nim przerw w działaniu usługi będzie traktowane jako nienależyte wykonanie umowy objętej gwarancją.   5.3. Poufność i ochrona danych   * + Dostawca zobowiązany jest do zachowania poufności wszelkich danych Zamawiającego.   + Wszelkie dane gromadzone w ramach usługi muszą być przechowywane i przetwarzane na terenie Unii Europejskiej.   + Wymagane jest pełne dostosowanie do przepisów RODO.   **6. Wymagania dla wykorzystywanych narzędzi**  **6.1 SIEM**   1. System zapewnia zbieranie, analizę, korelację, przechowywanie i wizualizację zdarzeń bezpieczeństwa oraz automatyczną reakcję na incydenty. System wspiera ocenę zgodności z regulacjami branżowymi i prawnymi, integruje się z różnymi źródłami danych oraz działa w środowiskach on-premises, chmurowych i kontenerowych. 2. System musi umożliwiać centralne gromadzenie zdarzeń z wielu źródeł oraz ich korelację w celu identyfikacji incydentów bezpieczeństwa. 3. System musi umożliwiać definiowanie i dostosowywanie reguł korelacyjnych. 4. System musi wspierać detekcję anomalii, ataków i zdarzeń krytycznych w oparciu o reguły i wzorce znanych zagrożeń. Wymagane jest mapowanie zdarzeń do taksonomii MITRE ATT&CK. 5. System musi składać się z komponentu zbierającego dane (agent), centralnego serwera analitycznego, modułu indeksującego oraz interfejsu administracyjno-wizualizacyjnego. 6. Rozwiązanie musi pracować w dwóch trybach pracy: agentowym oraz bezagentowym. 7. Bezagentowy tryb pracy musi umożliwiać monitorowanie bez instalacji agenta w powłoce systemu operacyjnego źródła danych (np. poprzez protokół SSH) z konfiguracją po stronie konsoli zarządzającej. 8. Agent musi przekazywać zdarzenia do serwera przez połączenie TCP. 9. Rozwiązanie musi wspierać klastrowanie dla skalowalności, równoważenia obciążenia i wysokiej dostępności; wymagane są procedury zarządzania klastrem i ILM (Index Lifecycle Management). 10. Rozwiązanie musi umożliwiać skalowanie horyzontalne przez dołączanie węzłów serwera i indexera; agenci mogą łączyć się przez LB/failover, a dane konfiguracyjne/reguły muszą być synchronizowane w klastrze. 11. Agent musi być dostępny dla systemów Linux, Windows, macOS. 12. Serwer musi działać na 64-bitowych CPU x86\_64/ARM64 i wspierać wskazane wersje dystrybucji Linux (m.in. RHEL 7–10, Ubuntu 16.04–24.04). 13. Wymagane są opcje wdrożenia on-prem, kontenery/Kubernetes. 14. System musi zbierać logi z wielu źródeł: agent (logcollector, event channel/eventlog Windows), urządzenia sieciowe/syslog, integracje chmurowe (AWS/Azure/GCP) oraz zewnętrzne API. 15. System musi obsługiwać integracje z usługami katalogowymi (np. Active Directory) oraz logami bezpieczeństwa systemów operacyjnych Windows (event channel). 16. Wymagane dekodowanie i reguły korelacyjne po stronie serwera analitycznego z możliwością testowania nowych reguł. 17. Agent powinien zapewniać funkcje monitorowania integralności plików, funkcje audytu oprogramowania z użyciem treści CTI (NVD/OVAL itp.), z opcją pracy w trybie offline oraz funkcję walidacji konfiguracji systemu operacyjnego w ramach, których dostawca zapewni gotowe polityki CIS dla systemów i aplikacji. 18. Rozwiązanie zapewni zestaw reguł ze wsparciem raportowania pod PCI DSS, HIPAA, NIST 800-53, TSC oraz GDPR (dedykowane panele). 19. Komponent indeksujący musi zapewniać pełnotekstowe wyszukiwanie, shardy/replice oraz polityki cyklu życia indeksów (ISM) dla kontroli retencji i wydajności. 20. Rozwiązanie zapewni wskaźniki zdrowia klastra i alokacji przestrzeni poprzez API Indexera. 21. Dashboard i API muszą udostępniać RBAC z precyzyjnymi uprawnieniami do zasobów/endpointów (role, reguły, polityki). 22. Wymagane jest otwarte REST API dla Managera i Indexera (operacje m.in. na agentach, klastrze, indeksach, zapytaniach). 23. Musi istnieć mechanizm tworzenia użytkowników (również „read-only”) i mapowania ról z poziomu Dashboard. 24. Kanały agent-server muszą być uwierzytelnione i szyfrowane (AES/alternatywy wg konfiguracji), z obsługą weryfikacji tożsamości agenta przez certyfikaty (SSL) w procesie enrolmentu. 25. Rozwiązanie musi zapewniać akcje skryptowe stateful/stateless realizowane po stronie źródła danych w przypadku wystąpienia określonego zdarzenia bezpieczeństwa. 26. Rozwiązanie powinno klasyfikować każde zdarzenie bezpieczeństwa do MITRE ATT&CK. 27. Interfejs administracyjny musi udostępniać pulpity menedżerskie, widoki operacyjne i raporty zgodności. 28. Musi istnieć możliwość tworzenia i harmonogramowania raportów okresowych. 29. System musi udostępniać moduł zarządzania użytkownikami z podziałem na role i uprawnienia. 30. Musi istnieć możliwość definiowania użytkowników z ograniczonymi uprawnieniami (np. read-only). 31. System musi posiadać moduł monitorowania procesów uruchamianych w systemach operacyjnych oraz zdolność do wykrywania anomalii w ich zachowaniu. 32. Musi istnieć możliwość wykrywania eskalacji uprawnień w systemach operacyjnych. 33. System musi wspierać detekcję ataków typu brute-force, nieautoryzowanych logowań i manipulacji rejestru systemowego. 34. System musi posiadać moduł detekcji rootkitów na systemach Linux. 35. System musi udostępniać mechanizm centralnego zarządzania konfiguracją agentów. 36. System musi wspierać automatyzację wdrożeń poprzez narzędzia typu Ansible oraz instalacje kontenerowe.   Wymagania techniczne   1. System musi składać się z agenta, serwera analitycznego, modułu indeksującego oraz interfejsu wizualizacyjnego. 2. System oparty na architekturze rozproszonej (wieloserwerowej) z możliwością skalowania poziomego. 3. System musi wspierać klastrowanie serwera i modułu indeksującego w celu zapewnienia HA i skalowalności. 4. Kanały agent - serwer muszą być szyfrowane i uwierzytelnione. 5. Agent musi być dostępny dla Linux, Windows, macOS. Integracja z Active Directory/LDAP do zarządzania użytkownikami. 6. Możliwość pracy w trybie HA (High Availability). 7. Zabezpieczenie transmisji danych (TLS/SSL). 8. Możliwość przechowywania danych w środowisku on-premise lub w chmurze zgodnej z wymogami RODO. 9. Komponenty centralne muszą być możliwe do wdrożenia w środowiskach on-prem, kontenerowych i chmurowych. 10. System musi zapewniać pełnotekstowe wyszukiwanie zdarzeń. 11. System musi udostępniać REST API do zarządzania agentami, danymi i klastrem. 12. Interfejs musi wspierać kontrolę dostępu opartą o role. 13. System musi udostępniać centralne zarządzanie konfiguracją agentów.   Wymagania dotyczące utrzymania i wsparcia   1. Dostawca zapewni wsparcie techniczne w trybie 24/7 dla incydentów krytycznych. 2. Regularne aktualizacje systemu i reguł bezpieczeństwa. 3. Szkolenia administratorów i analityków SOC z obsługi systemu. 4. Dokumentacja techniczna i użytkowa w języku polskim.   Integracja i rozwój   1. Integracja z systemami bezpieczeństwa Zamawiającego: firewalle, IPS/IDS, EDR/XDR, systemy antywirusowe, systemy zarządzania podatnościami. 2. Integracja z narzędziami orkiestracji i automatyzacji (SOAR). 3. Możliwość eksportu danych do zewnętrznych repozytoriów i systemów raportowych. 4. Elastyczność w zakresie rozbudowy systemu o dodatkowe moduły i funkcje.   **8.2 SOAR**   1. System stanowi centralny komponent warstwy operacyjnej SOC. Integruje się z systemami źródłowymi (logi, zdarzenia, alerty), umożliwia automatyczne i manualne reakcje na incydenty oraz utrzymuje pełną historię działań. 2. System powinien być utrzymywany w zasobach Operatora usługi. 3. System musi być możliwy do instalacji na popularnych, wspieranych dystrybucjach serwerowych Linux (np. RHEL i jego pochodne, Ubuntu Server, SUSE) lub być dostarczany w formie zwirtualizowanego urządzenia (appliance) lub jako usługa SaaS. 4. Środowisko musi umożliwiać uruchomienie w trybie zgodnym z FIPS; jeśli wdrażane w trybie FIPS, jądro OS musi być uruchomione w trybie FIPS, a wszystkie węzły i składowe komunikować się zgodnie z wymogami FIPS. 5. System musi być wyposażony w webowy interfejs użytkownika z wsparciem komunikacji TLS 1.2/1.3; przy wdrożeniu na RHEL 8.x wszystkie aplikacje/ konektory/zasoby łączące się z systemem muszą używać co najmniej TLS 1.3. 6. Środowisko musi wspierać horyzontalne skalowanie poprzez klaster co najmniej trzech węzłów systemu oraz dedykowany load balancer; klaster zapewnia zarówno zwiększenie przepustowości jak i redundancję. 7. Konfiguracja HA musi obejmować replikację warstwy danych operacyjnych (baza/artefakty/vault) zgodnie z zaleceniami producenta oraz monitorowanie zdrowia węzłów. 8. System musi obsługiwać zdarzenia (kontenery) jako jednostki sprawy/śledztwa zawierające artefakty (dowody) w formacie JSON (w tym nagłówki CEF), na których operują playbooki oraz funkcje automatyzacji. 9. System musi zapewniać skarbiec plików (vault) powiązany ze zdarzeniami, z możliwością bezpiecznego dodawania/odczytu przez API i playbooki oraz kontrolą pojemności. 10. Playbooki muszą być tworzone w Pythonie 3 z wykorzystaniem dostarczonego runtime i API automatyzacji; integracje (aplikacje/konektory) muszą być zgodne z nowym runtime i polityką pakietów. 11. System musi wspierać REST API dla wszystkich zasobów systemu (m.in. kontenery, artefakty, vault) z operacjami CRUD i filtrowaniem. 12. System musi obsługiwać model kontenerów i artefaktów jako podstawowych jednostek danych. 13. System musi zapewniać bezpieczny vault do przechowywania plików związanych z kontenerami. 14. System powinien zapewniać edytor oraz SDK do tworzenia automatyzacji. 15. Automatyczne klasyfikowanie i priorytetyzacja incydentów bezpieczeństwa. 16. Obsługa pełnego cyklu życia incydentu: rejestracja, analiza, reakcja, zamknięcie. 17. Możliwość przypisywania incydentów do konkretnych analityków lub zespołów. 18. Historia działań i logowanie wszystkich operacji w ramach incydentu. 19. Mechanizmy eskalacji incydentów zgodnie z polityką bezpieczeństwa Zamawiającego. 20. System musi umożliwiać obsługę zdarzeń w formacie JSON, w tym nagłówków CEF.   Integracje   1. Gotowe konektory do popularnych systemów bezpieczeństwa - Fortinet, używanego przez Zamawiającego . 2. Możliwość tworzenia własnych konektorów (Custom Apps/Connectors). 3. Integracja z systemami ITSM (np. ServiceNow, Jira) w celu obsługi zgłoszeń. 4. Obsługa API REST do wymiany danych z innymi systemami.   Playbooki i automatyzacja reakcji   1. Predefiniowane playbooki dla typowych incydentów (np. phishing, malware, ransomware, brute force). 2. Możliwość budowy złożonych procesów obejmujących wiele systemów. 3. Obsługa interaktywnych akcji wymagających zatwierdzenia przez analityka. 4. Wizualizacja przebiegu playbooków i statusów ich realizacji. 5. System musi obsługiwać równoległe wykonywanie wielu playbooków.   Analiza i raportowanie   1. Dashboardy prezentujące status incydentów, czas reakcji, skuteczność playbooków. 2. Raporty okresowe (miesięczne, kwartalne, roczne). 3. Analiza efektywności automatyzacji (KPI: MTTD – Mean Time to Detect, MTTR – Mean Time to Respond). 4. Raporty zgodności z regulacjami (RODO, NIS2, KSC, ISO 27001). 5. W systemie musi istnieć mechanizm audytu, historii działań i raportowania.   Wymagania techniczne   1. Architektura systemu umożliwiająca skalowanie horyzontalne. 2. Możliwość pracy w trybie HA (High Availability). 3. Wsparcie dla instalacji on-premise, w chmurze publicznej lub hybrydowej. 4. Interfejs webowy w języku angielskim; dokumentacja i wsparcie w języku polskim. 5. Autoryzacja użytkowników z wykorzystaniem SSO (Single Sign-On), LDAP/Active Directory. 6. Obsługa mechanizmów wieloskładnikowego uwierzytelnienia (MFA). 7. Wymuszenie szyfrowania komunikacji (TLS 1.2+).   **8.3 Wymagania dla systemu do zarządzania podatnościami**  8.3.1.Zarządzanie projektami skanowanie podatności i testów penetracyjnych   1. Tworzenie i zarządzanie projektami od etapu planowania po końcowe raportowanie. 2. Obsługa wielu projektów równolegle z możliwością przypisywania zespołów i ról (kierownik projektu, tester, analityk). 3. Harmonogramowanie testów i monitorowanie ich postępów. 4. Rejestrowanie komunikacji i wymiany informacji z dostawcami usług testów penetracyjnych.   8.3.2. Analiza wyników testów   1. Automatyczne importowanie i analiza wyników z narzędzi do testów penetracyjnych (np. Burp Suite, Nessus, Metasploit, Nmap). 2. Kategoryzacja wyników według poziomu krytyczności, rodzaju podatności, systemu i aplikacji. 3. Prezentacja wyników w podziale na etapy testów: information gathering, identyfikacja podatności, exploitation. 4. Generowanie rekomendacji działań naprawczych w języku polskim   8.3.3. Raportowanie i wizualizacja   1. Tworzenie raportów w formacie DOCX, 2. Raporty dostosowane do odbiorców technicznych (szczegóły techniczne, dowody exploitacji) i nietechnicznych (zarząd, compliance). 3. Wbudowane dashboardy prezentujące status testów, ilość i typy podatności, trendy w czasie. 4. Możliwość personalizacji raportów i ich automatycznej dystrybucji.   8.3.4. Archiwizacja i analiza historyczna   1. Archiwizacja wyników testów w bezpiecznej bazie danych. 2. Możliwość porównania wyników testów z różnych okresów i projektów. 3. Analiza trendów w podatnościach – identyfikacja nawracających problemów. 4. Wsparcie dla tworzenia planów długoterminowych działań naprawczych.   8.3.5. Integracja i współpraca   1. Integracja z narzędziami skanującymi i testującymi (Nessus, OpenVAS, Burp, OWASP ZAP). 2. API REST umożliwiające integrację z innymi systemami bezpieczeństwa i raportowania.   8.3.6 Wymagania techniczne   1. Wsparcie dla systemów Linux i Windows. 2. Dostęp przez przeglądarkę (interfejs webowy responsywny, UX-friendly). 3. Szyfrowanie danych w spoczynku i w transmisji (TLS 1.2+, AES-256).   8.3.7. Wymagania dotyczące użytkowników i ról   1. Możliwość definiowania ról: administrator, kierownik projektu, tester, analityk, audytor. 2. Granularne zarządzanie uprawnieniami (RBAC). 3. Historia i audyt działań użytkowników.   8.3.8. Wymagania raportowe i zgodności   1. Raporty zgodne z wymaganiami regulacyjnymi: RODO, NIS2, KSC, ISO 27001. 2. Eksport danych w formatach CSV, JSON, XML. 3. Audyt działań i zgodność z polityką bezpieczeństwa organizacji. |

## EDR

|  |
| --- |
| Przedmiotem zamówienia jest dostawa **terminowych licencji** zaawansowanego systemu cyberbezpieczeństwa klasy EDR/EPP, realizowanego w architekturze z centralną konsolą zarządzającą (dostępną w modelu SaaS).  Zamawiający wymaga dostarczenia licencji w modelu **pre-paid (opłaconym z góry)** na okres **36 miesięcy**.  Cena ofertowa musi być ceną ryczałtową i obejmować prawo do korzystania z oprogramowania, wszystkich jego modułów, aktualizacji sygnatur, aktualizacji wersji agentów oraz wsparcia technicznego producenta przez pełny okres 3 lat.  Zamawiający nie dopuszcza modelu, w którym płatność jest rozłożona na raty lub abonamenty miesięczne/roczne.  Wraz z dostawą Wykonawca zobowiązany jest przekazać **Certyfikat Licencyjny** (lub równoważny dokument wystawiony przez producenta systemu), potwierdzający, że:   * Licencje zostały opłacone u producenta na pełny okres 36 miesięcy z góry. * Data wygaśnięcia wsparcia i subskrypcji przypada nie wcześniej niż za 36 miesięcy od daty aktywacji. * Zamawiający jest uprawniony do bezpośredniego korzystania ze wsparcia producenta, niezależnie od dalszego istnienia Wykonawcy.   System musi przetwarzać i przechowywać dane telemetryczne w chmurze zlokalizowanej na terenie Europejskiego Obszaru Gospodarczego (EOG) i być zgodny z RODO.  System powinien oferować centralną konsolę zarządzania, wysoką dostępność (co najmniej 99,9%) oraz wsparcie dla szerokiej gamy urządzeń, w tym serwerów, stacji roboczych i urządzeń mobilnych.  Wszystkie moduły i funkcje muszą pochodzić od jednego producenta, a dane przetwarzane w systemie muszą być zgodne z regulacjami GDPR oraz standardami bezpieczeństwa, takimi jak ISO/IEC 27001:2022 i SOC 2 Type 2.  System musi zapewniać retencję danych telemetrycznych i logów przez minimum 365 dni oraz oferować szerokie możliwości automatyzacji, takie jak grupowanie alertów, tworzenie scenariuszy obsługi incydentów oraz integrację z narzędziami zewnętrznymi poprzez interfejs API.  **Wymagania ogólne**   1. System musi posiadać centralną konsolę realizowaną w formie usługi SaaS (ang. Software-as-a-Service) o dostępności co najmniej 99,9%, a do ochrony stacji i serwerów wykorzystywać agenta. 2. Wszystkie moduły funkcjonalne systemu muszą być dostarczony od jednego producenta. 3. System musi przechowywać i przetwarzać dane na terenie Europejskiego Obszaru Gospodarczego. 4. System musi być zgodny z regulacjami GDPR (ang. General Data Protection Regulation), posiadać certyfikację ISO/IEC 27001:2022 oraz lub zgodność z SOC 2 Type 2. 5. **System należy dostarczyć z subskrypcją na okres 36 miesięcy umożliwiającą objęcie ochroną ilości serwerów i stacji roboczych wskazanych w opisie zamówienia podstawowego lub prawa opcji.** 6. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 dni. 7. System musi przechowywać szczegółowe dane telemetryczne z chronionych systemów w taki sposób, aby możliwe było ich manualne przeszukiwania w konsoli systemu oraz przez interfejs API. Nie dopuszcza się, aby system posiadał jakiekolwiek ograniczenia licencyjne na manualne przeszukiwania w/w danych z konsoli. 8. Interfejs API systemu musi umożliwiać co najmniej następujące akcje:    1. Wykonanie kwerendy do danych telemetrycznych z endpointa i z systemów trzecich    2. Pobranie pliku instalacyjnego agenta    3. Uruchomienie skryptu na wskazanym hoście    4. Zarządzenia izolacją sieciową danego hosta    5. Przywrócenie pliku z kwarantanny    6. Pobranie informacji o alarmach    7. Zlecenie skanowania hosta    8. Pobranie pliku z hosta 9. System musi przechowywać przez 365 dni logi audytowe odnotowujące co najmniej logowanie użytkowników, zmiany wprowadzane w konfiguracji systemu, nawiązywanie zdalnych połączeń do chronionych stacji i wykorzystanie interfejsu API. 10. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:     1. Microsoft:     * Windows 11 (x86-64 oraz arm64)     * Windows 10 (x86-64 oraz arm64)     * Windows 7 SP1     * Windows Server 2008 R2 SP1     * Windows Server 2012 i 2012 R2     * Windows Server 2016 i Server Core 2016     * Windows Server 2019 i Server Core 2019     * Windows Server 2022 i Server Core 2022     * Windows Server 2025 i Server Core 2025     1. Linux     * Debian 10, 11 i 12     * Oracle Linux 8 i 9     * Red Hat Enterprise Linux 8, 9 i 10     * Rocky Linux 8, 9 i 10     * SUSE 11, 12 i 15     * Ubuntu 18, 20, 22 i 24     1. Apple macOS     * macOS Ventura 13     * macOS Sonoma 14     * macOS Sequoia 15     * macOS Tahoe 26     1. Apple iOS/iPadOS od 16.x do 18.x     2. Android od 9.x do 15.x 11. System musi posiadać możliwość instalacji agenta na systemach Windows 7 SP1 nie objętych rozszerzonym wsparciem producenta. Wersja agenta dla w/w systemu operacyjnego nie może być wycofana ze wsparcia Producenta, aby otrzymywać bieżące aktualizacje mechanizmów detekcyjno-prewencyjnych. 12. System musi posiadać możliwość instalacji agenta na systemach VDI. 13. System musi umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:     * W formacie msi lub exe dla systemów Microsoft     * W formacie pakietu rpm i deb dla systemów Linux     * W formacie pakietu pkg dla macOS 14. System musi umożliwiać instalację agenta dla systemów iOS/iPadOS i Android za pośrednictwem systemu MDM lub odpowiednio ze sklepu Apple Store i Google Play. 15. Komunikacja między agentem a konsolą systemu musi być realizowana z wykorzystaniem protokołu HTTPS w wariancie co najmniej z TLS1.2 i odbywać się:     * Bezpośrednio     * Pośrednio przez proxy systemowe     * Pośrednio przez proxy wskazane w trakcie instalacji 16. Dokumentacja systemu musi wskazywać adresy IP oraz adresy URL, z którymi komunikuje się agent nawiązując komunikację z konsolą systemu, aby umożliwić udrożnienie komunikacji sieciowej. 17. System musi posiadać możliwość zarządzania przez przeglądarkę internetową. Komunikacja musi być zabezpieczona HTTPS w wariancie co najmniej z TLS1.2. 18. Interfejs webowy systemu nie może korzystać z komponentów typu Flash, Silverlight, applet Java, ActiveX, wtyczek NPAPI. 19. System musi posiadać możliwość zarządzania przez interfejs API. Uwierzytelnienie do interfejsu API platformy musi być realizowane w oparciu o OAuth2 i musi oferować możliwość granularnej autoryzacji dostępu klienta OAuth2 do poszczególnych obszarów funkcjonalnych Systemu. 20. System musi posiadać możliwość wskazania listy publicznych adresów IP, z których będzie istniała możliwość zalogowania się do konsoli systemu oraz nawiązania połączenia do interfejsu API. 21. System musi umożliwiać integrację z zewnętrznymi katalogami użytkowników z wykorzystaniem SAML 2.0. 22. System musi posiadać wbudowany katalog użytkowników oraz obsługiwać drugi czynnik uwierzytelniający wykorzystujący tokeny TOTP (ang. Time Based One-Time Password). 23. System podczas tworzenia haseł dla lokalnych kont administracyjnych musi wymuszać minimalnie następujące wymagania złożoności hasła: co najmniej 11 znaków, musi zawierać małe i duże litery, cyfry i znaki specjalne. 24. System nie może posiadać ograniczenia licencyjnego na liczbę użytkowników (administratorów, analityków, inżynierów bezpieczeństwa) zdefiniowanych w systemie ani ograniczenia na równocześnie zalogowanych w systemie użytkowników. Wszyscy użytkownicy muszą posiadać własne konta imienne. Nie dopuszcza się wykorzystania współdzielonych kont użytkowników. 25. System musi umożliwiać określenie zakresu dostępu z wykorzystaniem matrycy ról i ich przypisania do użytkownika lub do grupy użytkowników. Rola musi definiować dostęp do określonego obszaru administracyjnego systemu, jego rodzaj (tylko do odczytu, pełen dostęp) oraz jego zakresu (wszystkie lub wybrane hosty). 26. System musi obsługiwać co najmniej 5 poziomów ważności alarmów, np: informacyjny, niski, średni, wysoki i krytyczny. 27. System musi automatycznie grupować powiązane alerty w celu przyspieszenia i ułatwienia triażu i analizy incydentu. 28. System musi umożliwiać tworzenie wyjątków dla reguł prewencyjnych na podstawie certyfikatu producenta oprogramowania. 29. System dla alarmów zgrupowanych w ramach incydentu musi automatycznie tworzyć łańcuchy przyczynowo skutkowe reprezentujące zależności pomiędzy procesami wykorzystywanymi w trakcie ataku i powiązane dane telemetryczne, celem ułatwienia przeanalizowania wykorzystywanych technik, określenia zakres ataku, ustalenia celu i zakresu ataku oraz zweryfikowania, czy atak się powiódł. 30. System musi umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:     * Przypisanie incydentu do analityka     * Zmianę stanu incydentu np: badany, false positive, true positive, duplikat, testy     * Dodawanie notatek 31. System musi mapować alarmy do frameworku MITRE ATT&CK. 32. System musi posiadać konfigurowalną możliwość automatycznego uploadowania plików do analizy w sandboxie oraz umożliwiać upload do sandboxa arbitralnych próbek co najmniej przez interfejs API. Wymaga się dostarczyć licencję umożliwiającą upload co najmniej 250 próbek miesięcznie. 33. System musi umożliwiać wgląd w raport z sandboxa dla plików powiązanych z incydentem i eksport raportu. 34. System musi posiadać możliwość kontroli urządzeń podłączanych do portów USB co najmniej na systemach windows i macOS w następującym zakresie:     1. Określenia jakie urządzenia USB można podłączyć     2. Określenia zakresu dostępu do pamięci masowej USB:     * Brak dostępu     * Tylko odczyt     * Odczyt i zapis     * Odczyt, zapis i uruchamianie 35. System musi posiadać możliwość kontroli host firewalla co najmniej na systemach Windows, MacOS oraz Linux. 36. System musi posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta musi umożliwiać określenie: 37. Dnia tygodnia i zakresu czasu, w którym aktualizacja nie będzie wykonywana 38. Tempa propagacji aktualizacji 39. Możliwość wersji: względnie wobec najnowszych wydanych lub bezwzględnie (konkretna wersja) 40. System musi posiadać możliwość kontroli w jaki sposób agent będzie pobierał aktualizacje mechanizmów detekcyjno-prewencyjnych co najmniej w następującym zakresie:     * Agent pobiera aktualizację natychmiast po opublikowaniu przez producenta     * Agent pobiera aktualizację z określonym opóźnieniem od momentu publikacji przez producenta 41. System musi umożliwiać dynamiczne grupowanie hostów z wykorzystaniem co najmniej następujących atrybutów: nazwa hosta, domena i OU w Active Directory, system operacyjny, adres ip, podsieć ip, znacznik. 42. System musi umożliwiać nawiązanie zdalnego połączenia konsolowego do hosta chronionego agentem oferując co najmniej następujące funkcje:     1. Podgląd uruchomionych procesów     2. Podgląd systemów plików     3. Podgląd stanu socketów sieciowych     4. Wyłączenie wskazanego procesu     5. Uruchomienie skryptu z biblioteki     6. Pobranie pliku z hosta     7. Wgranie pliku na hosta     8. Zrzut pamięci procesu     9. Zrzut pamięci systemu operacyjnego     10. Wyłączenie i restart systemu 43. System musi umożliwiać zdalną izolację sieciową hosta. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany. 44. System musi umożliwiać tworzenie biblioteki skryptów oraz ich zdalne uruchamianie na pojedynczym hoście i na grupie hostów. Wymagana jest obsługa co najmniej następujących języków skryptowych:     * Systemy windows: powershell     * Systemy Linux: skrypty bash lub python     * Systemy MacOS: skrypty zsh lub python 45. System musi posiadać możliwość uruchomienia pełnego skanowania hosta na żądanie i w odpowiedzi na zarejestrowany alarm. 46. System musi umożliwiać integrację z zewnętrznymi bazami Threat Intelligence poprzez API lub wbudowane konektory, w celu wzbogacania kontekstu o reputację plików (np. typu VirusTotal), reputację domen i adresów IP (np. typu DomainTools) oraz ocenę ryzyka podmiotów (np. typu Security Scorecard). Wraz z Systemem nie jest wymagane dostarczenie licencji do żadnego z w/w narzędzi. 47. System musi umożliwiać globalne oraz per grupa hostów blokowanie uruchamiania plików binarnych poprzez wskazanie ich hasha. 48. System musi posiadać możliwość budowania własnych reguł detekcyjno-prewencyjnych bazujących co najmniej na określeniu łańcucha przyczynowo-skutkowego procesów wraz z określeniem parametrów linii poleceń. 49. System musi posiadać możliwość budowania własnych list indykatorów (ang. Indicator Of Compromise) w formie nazw domenowych, adresów IPv4 i IPv6 oraz hashy SHA256 i MD5 poprzez:     * Import indykatorów z pliku     * Manualne dodanie indykatorów     * Programowe dodanie indykatorów przez interfejs API 50. System musi umożliwiać definiowanie własnych dashboardów (konsol) z wykorzystaniem predefiniowanych widgetów (kontrolek) oraz kontrolek definiowanych samodzielnie poprzez kwerendy do danych telemetrycznych. 51. System musi umożliwiać przeszukiwanie wszystkich danych telemetrycznych przy pomocy kreatorów lub manualnie z wykorzystaniem kwerend. Kwerendy muszą umożliwiać łączenie danych telemetrycznych z różnych źródeł, ich filtrowanie, przekształcanie wyników i obsługiwać free text search (wyszukiwanie dowolnego ciągu znaków bez wskazywania konkretnego pola). Reguły tworzenia kwerend muszą być opisane w dokumentacji systemu. 52. System musi umożliwiać zapisanie kwerendy do danych telemetrycznych do biblioteki. 53. System musi umożliwiać zrealizowanie kwerendy do danych telemetrycznych i odczytanie jej wyników via interfejs API. 54. System musi umożliwiać eksport wyników kwerendy do danych telemetrycznych w formie pliku tekstowego. 55. System musi umożliwiać przekształcenie kwerendy do danych telemetrycznych w uruchamianą zgodnie z podanym harmonogramem regułę korelacyjną generującą alarmy, jeśli kwerenda zwróciła więcej niż jeden rekord. 56. System musi umożliwiać wykrywanie zasobów podłączonych w sieci wewnętrznej w sposób pasywny (analiza tablicy ARP) oraz umożliwiać skonfigurowanie aktywnego skanowania sieci. 57. System musi posiadać następujące możliwości przetwarzania logów z systemów trzecich:     1. Co najmniej 10GB logów dziennie     2. Wsparcie co najmniej dla następujących systemów     * Windows Event Logs     * firewalli Palo Alto Networks     * firewalli Fortinet     * Proofpoint Email Security     * Cisco Secure Email Gateway     * Apple macOS     * Microsoft Azure Event Hubs     * Microsoft Exchange Online     * Microsoft Graph API     * ZScaler     * Uniwersalny Http Event Collector lub podobny 58. System musi umożliwiać eksport danych telemetrycznych z agenta i danych telemetrycznych z systemów trzecich. 59. System musi posiadać wbudowany moduł SOAR (ang. Security Orchestration, Automation and Response) umożliwiający automatyczną obsługę alarmów w tym m.in. możliwość zmiany konfiguracji (orkiestracji) innych systemów bezpieczeństwa i rozszerzenie kontekstu alarmu poprzez integrację z systemami trzecimi. Wbudowany moduł SOAR musi umożliwiać budowanie spersonalizowanych scenariuszy obsługi (ang. playbooki) z wykorzystaniem graficznego narzędzia bez potrzeby pisania kodu. 60. Wbudowany moduł SOAR musi posiadać możliwość orkiestracji systemów bezpieczeństwa wewnątrz sieci Zamawiającego (systemów on-prem) oraz systemów bezpieczeństwa dostarczanych w formie usługi chmurowej (systemy SaaS). 61. Wszystkie moduły funkcjonalne systemu muszą być dostarczone z takim samym okresem licencji tj. na okres 36 miesięcy.   **Wymagania dla agenta**   1. Agent nie może wykorzystywać Oracle Java JRE/JDK. 2. Instalacja agenta nie może wymagać restartu systemu operacyjnego. 3. Agent musi weryfikować poprawność certyfikatu w trakcie nawiązywania połączenia z systemem w celu ochrony przed atakami man-in-the-middle z wykorzystaniem mechanizmu certificate pinning lub podobnego. 4. Agent musi posiadać mechanizmy ochronne uniemożliwiające wyłączenie agenta lub wpłynięcie na jego poprawne funkcjonowanie nawet przez użytkowników z podwyższonymi uprawnieniami (ang. anti-tampering) na systemach Windows, macOS i Linux. 5. Odinstalowanie agenta musi być chronione unikalnym hasłem dla każdej chronionej stacji, tak aby uniemożliwić odinstalowanie agenta nawet użytkowników z podwyższonymi uprawnieniami na systemach Windows, macOS i Linux. 6. W trakcie instalacji agenta musi istnieć możliwość nadania agentowi nieusuwalnego bezpośrednio z konsoli systemu znacznika, który może zostać wykorzystany jako atrybut do grupowanie hostów. 7. W trakcie instalacji agenta musi istnieć możliwość wskazania dedykowanego serwera proxy, z którego agent będzie korzystał nawiązując połączenie z systemem. 8. Agent musi wykrywać i blokować próby wyłączenia usługi Volume Shadow Copy Service (VSS) oraz inne próby uszkodzenia migawek VSS. 9. Agent musi realizować ochronę przed atakami klasy Bring Your Own Vulnerable Driver poprzez wykrywanie i blokowanie prób ładowania podatnych sterowników. 10. Agent musi bezpośrednio na chronionym hoście zapewniać ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi co najmniej w następujący sposób:     * Weryfikacja reputacji pliku w bazie threat intelligence producenta systemu     * Lokalna analiza statyczna bazująca na uczeniu maszynowym (ang. Machine learning) 11. Agent musi zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami w plikach Microsoft Word i Microsoft Excel co najmniej w następujący sposób:     * Weryfikacja reputacji makra w bazie threat intelligence producenta     * Lokalna analiza statyczna bazująca na uczeniu maszynowymi (ang. Machine learning) 12. Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel. 13. Agent musi realizować ochronę przed zaszyfrowaniem dysku i plików przez złośliwe oprogramowanie (aka ochrona anty-ransomware’owa). 14. Agent musi wykonywać analizę plików binarnych po tym jak zostały zapisane w systemie plików. 15. Musi zapewniać ochronę przed znanymi i nieznanymi exploitami wykorzystującymi znane i nieznane luki bezpieczeństwa w oprogramowaniu. 16. Agent musi posiadać konfigurowalną opcję umieszczania złośliwych plików w kwarantannie. 17. Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB lub musi blokować próby intencjonalnego i automatycznego uruchomienia plików wykonywalnych z pamięci masowej. 18. Agent musi posiadać mechanizm skanowania pamięci RAM w celu wykrywania złośliwego kodu. 19. Agent, poprzez analizę złożonych łańcuchów przyczynowo skutkowych i wykrywanie technik i taktyk stosowanych przez cyberprzestępców, musi zapewnić ochronę przed atakami klasy Living of The Land wykorzystującymi legalne narzędzia systemowe w groźny sposób. 20. Agent musi zapewniać ochronę przed atakami mającymi na celu kradzież poświadczeń użytkowników. 21. Agent musi posiadać możliwość automatycznej remediacji złożonych ataków co najmniej poprzez wyłączenie złośliwych procesów, umieszczenie plików w kwarantannie, usunięcie zadań z harmonogramu i wpisów z rejestru. 22. Agent musi integrować się z Windows Security Center. 23. Agent musi umożliwiać kwarantannę groźnych plików. 24. Agent musi działać:     * W jądrze systemu (używać sterownika) na systemach Windows     * W jądrze systemu (aka kernel space) lub poza jądrem systemu (aka user space) na systemach Linux     * Poza jądrem systemu na systemach MacOS 25. Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:     1. Utworzenie nowego procesu i zakończenie procesu     2. Operacje na socketach sieciowych dla TCP i UDP     3. Operacje na plikach     4. Zdarzenia z event logu dotyczące uwierzytelnienia.     5. Operacje na rejestrze (tylko systemy Windows) 26. W przypadku braku łączności z systemem agent musi lokalnie przechować dane telemetryczne i wysłać je do systemu po przywróceniu łączności sieciowej. ` |
| **Dodatkowe kryteria oceny ofert**  ***Spełnienie poniższych kryteriów pozwoli na otrzymanie dodatkowych punktów w trakcie oceny.***   1. Dodatkowo ochrona MFA dla nawiązywania połączenia zdalnego   System przed nawiązaniem zdalnego połączenia konsolowego musi żądać od administratora ponownego wprowadzenia hasła MFA celem dodatkowego potwierdzenia jego tożsamości w celu podwyższenia odporności systemu na ataki wynikające z kradzieży tożsamości.   1. Wbudowany Cyber Threat Intelligence   System musi powiązywać, tam, gdzie atrybucja jest możliwa, indykatory IOC, techniki i procedury z konkretną grupą cyber przestępczą / grupą APT / grupą haktywistyczną. |

## Przygotowanie, wdrożenie i utrzymanie procedur związanych z SZBI (Security Officer)

|  |
| --- |
| Celem zamówienia jest zaprojektowanie, udokumentowanie i wsparcie wdrożenia w strukturach Zamawiającego (Szpital w Katowicach) spójnego i funkcjonalnego Systemu Zarządzania Bezpieczeństwem Informacji (SZBI). System ten ma na celu zapewnienie poufności, integralności i dostępności informacji, a także osiągnięcie i utrzymanie zgodności z kluczowymi regulacjami prawnymi i normami.  **Kluczowe podstawy normatywne i prawne:**  Opracowany i wdrożony SZBI musi być w pełni zgodny z wymaganiami następujących dokumentów (w ich najnowszych, obowiązujących na dzień udzielenia zamówienia wersjach):   1. Norma ISO/IEC 27001 - "Information security, cybersecurity and privacy protection — Information security management systems — Requirements". 2. Norma ISO/IEC 27005 - "Information security, cybersecurity and privacy protection — Guidance on managing information security risks". 3. Norma ISO 22301 - "Security and resilience — Business continuity management systems — Requirements". 4. Norma PN-ISO/IEC 29134 – Wytyczne do przeprowadzenia oceny skutków dla prywatności (DPIA). 5. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. 6. Rozporządzenie Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności (KRI). 7. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (RODO). 8. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 (Dyrektywa NIS 2).  **Szczegółowy Zakres Prac** Realizacja zamówienia została podzielona na cztery logiczne, następujące po sobie etapy. Odbiór każdego etapu jest warunkiem koniecznym do rozpoczęcia kolejnego. **ETAP I: Audyt Zerowy i Analiza Luk**  1. **Przeprowadzenie diagnozy przedwdrożeniowej** w siedzibie Zamawiającego. 2. **Analiza dostępnej dokumentacji** wewnętrznej Zamawiającego (regulaminy, procedury, instrukcje) pod kątem ich wpływu na bezpieczeństwo informacji. 3. **Przeprowadzenie wywiadów** z kluczowym personelem (kadra zarządzająca, pracownicy IT, pracownicy medyczni i administracyjni) w celu zmapowania kluczowych procesów przetwarzania informacji. 4. **Weryfikacja i identyfikacja luk** w istniejących zabezpieczeniach (organizacyjnych, technicznych i fizycznych) w odniesieniu do każdego z wymagań aktów prawnych i norm wymienionych w pkt 2.2. 5. **Produkt/Deliverable:** Opracowanie i przekazanie Zamawiającemu **"Raportu z Audytu Zerowego"**, który musi zawierać:    * Streszczenie menedżerskie.    * Szczegółową analizę luk (Gap Analysis) z odniesieniem do konkretnych punktów norm i przepisów.    * Ocenę dojrzałości organizacji w obszarze bezpieczeństwa informacji.    * Rekomendacje działań naprawczych.    * Proponowany, zharmonizowany plan realizacji kolejnych etapów prac.  **ETAP II: Szacowanie i Analiza Ryzyka**  1. **Opracowanie i przedstawienie do akceptacji Zamawiającego metodyki analizy ryzyka**, zgodnej z normą ISO/IEC 27005.   **Wykonawca zobowiązany jest do uwzględnienia w planowanym szacowaniu, analizie i postępowaniu z ryzykami w zakresie bezpieczeństwa informacji, również specyfiki bezpieczeństwa danych osobowych i danych medycznych. Metodyka analizy ryzyka zgodna z normą ISO/IEC 27005, winna obejmować również kryterium ryzyka w oparciu o przepisy RODO. W tym przypadku winny być uwzględnione ryzyka dla praw i wolności osób fizycznych, a następnie zaproponowanie w uzgodnieniu z Administratorem odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo przetwarzania danych osobowych.**  **Wymaganie zawarte powyżej wynika z interpretacji i oceny Prezesa UODO, który nałożył kare w wysokości 66 500 zł na Uniwersytecki Dziecięcy Szpital Kliniczny im. L. Zamenhofa w Białymstoku za niewdrożenie odpowiednich środków technicznych i organizacyjnych.**  **Prezes UODO zwrócił uwagę w opublikowanym komunikacie dotyczącym nałożonej kary, że istnieją różnice pomiędzy cyberbezpieczeństwem a ochroną danych osobowych. Administrator powołał się w tej sprawie na przeprowadzony audyt zgodności z ustawą o krajowym systemie cyberbezpieczeństwa. Organ nadzorczy wskazał, że – mimo pewnych podobieństw – procedury cyberbezpieczeństwa i ochrony danych osobowych służą różnym celom. Celem wdrażania procedur związanych cyberbezpieczeństwem jest przede wszystkim zapewnienie niezakłóconego**  **i bezpiecznego świadczenia usług. Z kolei celem implementacji środków technicznych**  **i organizacyjnych, o których mowa w RODO, jest zapewnienie bezpieczeństwa danym osobowym przetwarzanym przez Administratora.**  **Spełnienie wymogów cyberbezpieczeństwa nie zawsze oznacza spełnienie wymogów ochrony danych**   1. **Wspólna z personelem Zamawiającego identyfikacja i inwentaryzacja aktywów** informacyjnych (dane, oprogramowanie, infrastruktura, ludzie). 2. **Klasyfikacja zidentyfikowanych aktywów** pod względem ich krytyczności (poufność, integralność, dostępność). 3. **Przeprowadzenie warsztatów szacowania ryzyka** z udziałem właścicieli procesów po stronie Zamawiającego, mających na celu identyfikację zagrożeń, podatności oraz ocenę poziomu ryzyka. 4. **Produkt/Deliverable:** Opracowanie i przekazanie Zamawiającemu kompletnej dokumentacji z analizy ryzyka, zawierającej:    * **Rejestr Aktywów Informacyjnych.**    * **Raport z Analizy Ryzyka**, zawierający zidentyfikowane ryzyka wraz z ich oceną.    * **Plan Postępowania z Ryzykiem**, określający sposób reakcji na każde zidentyfikowane ryzyko (akceptacja, mitygacja, transfer, unikanie).  **ETAP III: Opracowanie Dokumentacji Systemowej SZBI**  1. Na podstawie wyników Etapu I i II, Wykonawca opracuje kompletny zestaw dokumentacji SZBI. 2. **Kluczowy wymóg:** Wszystkie dokumenty muszą być opracowane w ścisłej współpracy z Zamawiającym i w pełni **dostosowane do specyfiki jego działalności, procesów (medycznych i administracyjnych), zasobów oraz infrastruktury**. Niedopuszczalne jest dostarczenie generycznych, niezaadaptowanych szablonów. Akceptacja dokumentacji będzie uzależniona od wykazania, że odnosi się ona do realnych, nazwanych procesów, zasobów i ról funkcjonujących u Zamawiającego. 3. **Minimalny zakres dokumentacji:**    * Księga SZBI (podręcznik systemu).    * Polityka Bezpieczeństwa Informacji.    * Deklaracja Stosowania (SoA).    * Polityka Ochrony Danych Osobowych (zgodna z RODO).    * Polityki szczegółowe, zasady i procedury obejmujące m.in.:      + Zarządzanie aktywami.      + Bezpieczeństwo osobowe (cykl życia pracownika).      + Zarządzanie uprawnieniami i dostępem.      + Bezpieczeństwo fizyczne i środowiskowe.      + Bezpieczeństwo teleinformatyczne (sieci, systemy, aplikacje).      + Zarządzanie incydentami bezpieczeństwa informacji.      + Zarządzanie ciągłością działania.      + Zasady zgodności z wymaganiami prawnymi i umownymi.    * Polityki i szczegółowe zasady i procedury winne również uwzględnić takie dokumenty jak:      + Polityka klasyfikacji informacji,      + Polityka zarządzania dostępem i uprawnieniami,      + Polityka zarządzania podatnościami,      + Polityka zarządzania ryzykiem z uwzględnieniem obszaru cyberbezpieczeństwa i przetwarzania danych osobowych,      + Polityka zarządzania incydentami cyberbezpieczeństwa i danych osobowych,      + Polityka zarządzania ciągłością działania z uwzględnieniem Planu Ciągłości Działania (BCP) oraz Plan Odzyskiwania po Awarii (Disaster Recovery Plan - DRP),      + Polityka logowania zdarzeń z uwzględnieniem aplikacji, sieci, serwerów, bramy brzegowej, kontrolera domeny,      + Procedura zarządzania dostawcami (zarządzania łańcuchem dostaw),      + Procedura zarządzania zmianami w urządzeniach i systemach IT,      + Procedura zarzadzania pojemnością i wydajnością krytycznych zasobów teleinformatycznych,      + Procedura zarządzania dokumentacja i zapisami SZBI,      + Procedura audytów wewnętrznych SZBI.    * Inne dokumenty (instrukcje, regulaminy, wzory oświadczeń), których potrzeba opracowania zostanie zidentyfikowana i uzasadniona na podstawie wyników Etapu I i II, po obustronnym pisemnym zatwierdzeniu przez Zamawiającego i Wykonawcę. 4. **Produkt/Deliverable:** Kompletna, zatwierdzona przez Zamawiającego **dokumentacja SZBI** w edytowalnej formie elektronicznej (np. format .docx).  **ETAP IV: Wsparcie Wdrożeniowe i Transfer Wiedzy**  1. **Przygotowanie dedykowanych materiałów szkoleniowych** dla różnych grup pracowników (kadra zarządzająca, personel IT, pracownicy medyczni, administracja). 2. **Aktywne wsparcie konsultacyjne i merytoryczne** dla zespołu Zamawiającego przy przeprowadzeniu pierwszego **audytu wewnętrznego SZBI**. 3. **Aktywne wsparcie konsultacyjne i merytoryczne** przy organizacji i przeprowadzeniu pierwszego **przeglądu zarządzania SZBI**. 4. **Produkt/Deliverable:**    * **Materiały szkoleniowe** w formie elektronicznej.    * **Protokół/raport z przeprowadzonych szkoleń** (zawierający program i listę uczestników).    * **Protokół/raport z audytu wewnętrznego** (opracowany wspólnie z zespołem Zamawiającego).    * **Protokół/raport z przeglądu zarządzania** (opracowany wspólnie z zespołem Zamawiającego).  **Kluczowe Wymagania i Warunki Realizacji**  1. Wykonawca jest zobowiązany do prowadzenia prac w taki sposób, aby zapewnić personelowi Zamawiającego transfer wiedzy umożliwiający samodzielne utrzymanie i doskonalenie SZBI po zakończeniu umowy. 2. Zamawiający zobowiązuje się do aktywnej współpracy z Wykonawcą, w tym do zapewnienia dostępu do niezbędnej dokumentacji, personelu oraz pomieszczeń w uzgodnionych terminach. 3. Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą "nie czyń poważnych szkód" (DNSH - Do No Significant Harm), co oznacza, że wdrożone rozwiązania nie mogą wywierać negatywnego wpływu na cele środowiskowe. 4. Odbiór każdego etapu będzie następował na podstawie protokołu zdawczo-odbiorczego, podpisanego bez uwag przez obie strony, po weryfikacji kompletności i jakości dostarczonych produktów (deliverables). Zamawiający ma 10 dni roboczych na zgłoszenie uwag do przekazanych materiałów. 5. Wszystkie produkty cyfrowe (w tym m.in. raporty, polityki, procedury, materiały szkoleniowe) wytworzone przez Wykonawcę w ramach realizacji zamówienia muszą spełniać standardy dostępności cyfrowej określone w dokumencie "Standardy dostępności dla polityki spójności 2021-2027", co jest równoznaczne ze spełnieniem wymagań ustawy z dnia 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych i zgodnością z wytycznymi Web Content Accessibility Guidelines (WCAG) 2.1 na poziomie AA |
| **Pakiet Nadzoru Autorskiego (Security Officer)**   1. W ramach zamówienia Wykonawca dostarczy Pakiet Nadzoru Autorskiego i Utrzymania (Maintenance SZBI) obejmujący okres 36 miesięcy. Przedmiotem tej części zamówienia nie jest świadczenie usługi ciągłej rozliczanej w okresach miesięcznych, lecz jednorazowy zakup pakietu gwarantującego utrzymanie aktualności dokumentacji, realizację przeglądów okresowych oraz gotowość konsultacyjną przez wymagany okres trwałości. 2. Okres realizacji Nadzoru Autorskiego rozpoczyna się w dniu następującym po dniu podpisania przez Zamawiającego bez uwag protokołu odbioru końcowego dla etapu wdrożenia SZBI (odbioru dokumentacji wdrożeniowej). 3. W ramach świadczenia Nadzoru SZBI, Wykonawca (działając w roli zewnętrznego "Security Officera") zobowiązany jest do:    1. **Proaktywnego monitorowania zmian w otoczeniu prawnym** (w szczególności zmian w ustawach, rozporządzeniach krajowych i unijnych, normach PN-ISO, komunikatach organów nadzorczych, np. CSIRT NASK, Prezesa UODO) mających wpływ na system bezpieczeństwa informacji Zamawiającego.    2. **Cyklicznych przeglądów aktualności dokumentacji SZBI**, przeprowadzanych **nie rzadziej niż raz na 12 (sześć) miesięcy**.    3. **Aktualizacji dokumentacji SZBI** wynikającej ze zidentyfikowanych zmian (o których mowa w lit. a) lub konieczności dostosowania dokumentacji do zmian organizacyjnych lub technicznych wprowadzanych przez Zamawiającego (np. wdrożenie nowych systemów IT, nowych zabezpieczeń, zmiana procesów przetwarzania informacji).    4. **Prowadzenia rokrocznych szkoleń** odnawiających wiedzę, zgodnie z wymogami normy dla kadry zarządzającej Zamawiającego.    5. Przeprowadzanie analizy ryzyka Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) nie rzadziej niż raz w roku oraz każdorazowo w przypadku istotnych zmian w systemie lub incydentów istotnie wpływających na poziom bezpieczeństwa. 4. **Tryb realizacji usługi:**    1. **Przeglądy (co 12 m-cy):** Każdy przegląd, o którym mowa w ust. 3 lit. b, zakończy się przekazaniem Zamawiającemu pisemnego (w formie elektronicznej) **„Raportu z Przeglądu SZBI”**. Raport musi zawierać co najmniej: wykaz zweryfikowanych dokumentów, opis zidentyfikowanych niezgodności lub luk (w odniesieniu do stanu faktycznego lub zmian prawnych) oraz rekomendacje lub projekt zmian w dokumentacji. Pierwszy przegląd musi odbyć się nie później niż 6 miesięcy od daty rozpoczęcia świadczenia Usługi Nadzoru SZBI.    2. **Aktualizacje (ad-hoc):**       1. W przypadku zidentyfikowania konieczności aktualizacji wynikającej ze zmian prawnych (ust. 3 lit. a), Wykonawca zobowiązany jest poinformować o tym Zamawiającego i przedstawić projekt zmian w dokumentacji w terminie nie dłuższym niż 30 dni od daty wejścia w życie danej zmiany.       2. W przypadku zgłoszenia przez Zamawiającego konieczności aktualizacji wynikającej ze zmian wewnętrznych (ust. 3 lit. c), Wykonawca zobowiązany jest dokonać analizy wpływu tej zmiany na SZBI i przedstawić projekt zmian w dokumentacji w terminie uzgodnionym z Zamawiającym, nie dłuższym niż 21 dni roboczych od daty zgłoszenia. 5. Wdrożenie (zatwierdzenie) zaktualizowanej dokumentacji przez Zamawiającego wymaga każdorazowo akceptacji Zamawiającego.   **Rozliczenie i Gwarancja Realizacji:**   1. Cena za Pakiet Nadzoru Autorskiego ma charakter ryczałtowy i obejmuje wszystkie koszty związane z utrzymaniem gotowości, aktualizacjami i przeglądami przez okres 36 miesięcy. 2. Podstawą do wystawienia faktury za Pakiet Nadzoru jest Protokół Odbioru Wdrożenia SZBI, potwierdzający dostarczenie pakietu i gotowość Wykonawcy do świadczenia nadzoru. 3. Niewykonanie przez Wykonawcę obowiązków objętych Pakietem (np. brak realizacji przeglądu co 6 miesięcy, brak aktualizacji dokumentacji w terminie 30 dni od zmiany przepisów) będzie traktowane jako **nienależyte wykonanie umowy objętej gwarancją**. 4. W takim przypadku Zamawiający uprawniony jest do naliczenia kar umownych oraz żądania zwrotu części wynagrodzenia proporcjonalnie do okresu, w którym nadzór nie był sprawowany należycie. |

## Szkolenia dla kadry kierowniczej z zakresu SZBI

|  |
| --- |
| **1. Cel i Kontekst Zamówienia**  1.1. Cel główny:  Celem zamówienia jest wyposażenie kadry kierowniczej Zamawiającego (Szpital w Katowicach) w wiedzę i kompetencje niezbędne do świadomego zarządzania ryzykiem w obszarze cyberbezpieczeństwa, rozumienia kluczowej roli i odpowiedzialności menedżerów w Systemie Zarządzania Bezpieczeństwem Informacji (SZBI) oraz podejmowania strategicznych decyzji chroniących dane pacjentów, ciągłość działania placówki oraz jej reputację.  1.2. Grupa docelowa:  Szkolenie jest przeznaczone dla kadry kierowniczej Szpitala, w tym m.in. Dyrekcji, Ordynatorów, Kierowników oddziałów i działów administracyjnych. Szacowana liczba uczestników: do 27 osób.  **2. Szczegółowy Zakres Przedmiotu Zamówienia**  Przedmiotem zamówienia jest kompleksowa organizacja i przeprowadzenie jednego, jednodniowego szkolenia stacjonarnego w formie warsztatu w siedzibie Zamawiającego.  2.1. Minimalny zakres merytoryczny szkolenia:  Wykonawca jest zobowiązany zrealizować szkolenie obejmujące co najmniej następujące moduły tematyczne:   * **Moduł 1: Krajobraz Zagrożeń – Dlaczego Szpital Jest Celem? (Perspektywa Menedżerska)**   + Omówienie cyberbezpieczeństwa jako ryzyka operacyjnego, finansowego i reputacyjnego.   + Analiza współczesnych ataków na placówki medyczne: ransomware, phishing, inżynieria społeczna, wycieki danych medycznych (ePHI) wraz z omówieniem realnych przypadków i ich konsekwencji.   + Moderowana dyskusja na temat identyfikacji kluczowych zagrożeń w procesach zarządzanych przez uczestników. * **Moduł 2: SZBI jako Narzędzie Zarządcze i Tarcza Ochronna**   + Wyjaśnienie roli i celu Systemu Zarządzania Bezpieczeństwem Informacji.   + Omówienie fundamentów prawnych i normatywnych z perspektywy odpowiedzialności kadry kierowniczej: ISO/IEC 27001, RODO, Ustawa o Krajowym Systemie Cyberbezpieczeństwa oraz Dyrektywa NIS2.   + Przedstawienie cyklu życia SZBI (PDCA) oraz roli i odpowiedzialności menedżera w tym procesie (odpowiedzialność za aktywa i ryzyka, promowanie polityk, zapewnienie zasobów). * **Moduł 3: Zarządzanie Ryzykiem – Od Teorii do Decyzji Biznesowych**   + Przedstawienie procesu szacowania ryzyka i jego wyników w sposób zrozumiały dla menedżerów.   + Nauka interpretacji mapy ryzyka.   + Omówienie strategii postępowania z ryzykiem (mitygacja, transfer, akceptacja, unikanie) na przykładach ryzyk specyficznych dla sektora zdrowia.   + Część warsztatowa: analiza 2-3 kluczowych ryzyk dla Szpitala i wypracowanie propozycji zarządczych decyzji mitygujących. * **Moduł 4: Lider w Sytuacji Kryzysowej – Zarządzanie Incydentem**   + Określenie roli kadry kierowniczej w procesie zarządzania incydentem bezpieczeństwa.   + Omówienie znaczenia Planów Ciągłości Działania (BCP) dla zapewnienia funkcjonowania jednostki w warunkach kryzysowych.   + Zasady komunikacji kryzysowej (wewnętrznej i zewnętrznej).   + Analiza scenariusza incydentu (np. atak ransomware) pod kątem kroków podejmowanych przez kadrę zarządzającą. * **Moduł 5: Budowanie Kultury Bezpieczeństwa – Podsumowanie i Dalsze Kroki**   + Rola menedżera jako lidera i promotora kultury bezpieczeństwa w organizacji.   + Przedstawienie praktycznych sposobów promowania świadomości w podległych zespołach.   + Sesja pytań i odpowiedzi.   **2.2. Wymagania organizacyjne:**   * **Forma:** Szkolenie musi być przeprowadzone w formie interaktywnego warsztatu stacjonarnego. * **Lokalizacja:** Siedziba Zamawiającego – Szpital w Katowicach. Zamawiający zapewni salę szkoleniową wyposażoną w rzutnik multimedialny. * **Czas trwania:** Minimum 5 godzin zegarowych (nie wliczając przerw). * **Termin realizacji:** Do uzgodnienia z Wykonawcą, jednak nie później niż do 60 dni od daty podpisania umowy. * **Materiały szkoleniowe:** Wykonawca jest zobowiązany przygotować i dostarczyć wszystkim uczestnikom materiały szkoleniowe w formie drukowanej oraz w edytowalnej wersji elektronicznej. * **Certyfikaty:** Wykonawca zapewni imienne certyfikaty ukończenia szkolenia dla wszystkich uczestników.   **3. Warunki Realizacji i Odbioru Zamówienia**  **3.1. Odbiór prac:** Odbiór przedmiotu zamówienia nastąpi po zrealizowaniu szkolenia, na podstawie protokołu zdawczo-odbiorczego podpisanego bez uwag przez obie strony. Warunkiem podpisania protokołu jest dostarczenie przez Wykonawcę:   * Listy obecności uczestników szkolenia. * Materiałów szkoleniowych w wersji elektronicznej. * Anonimowych ankiet ewaluacyjnych wypełnionych przez uczestników po zakończeniu szkolenia.   **3.2. Dostępność Cyfrowa:** Materiały szkoleniowe w wersji elektronicznej muszą spełniać standardy dostępności cyfrowej zgodne z wytycznymi WCAG 2.1 na poziomie AA. |

## Szkolenia dla personelu medycznego i administracyjnego z SZBI

|  |
| --- |
| **Cel i Przedmiot Zamówienia**   1. Celem zamówienia jest podniesienie świadomości i kluczowych kompetencji personelu medycznego i administracyjnego Zamawiającego w zakresie fundamentalnych zasad cyberbezpieczeństwa oraz wewnętrznych regulacji dotyczących bezpieczeństwa informacji. Realizacja zamówienia ma na celu wzmocnienie odporności organizacji na incydenty bezpieczeństwa poprzez edukację pracowników. 2. Szkolenie przeznaczone jest dla personelu medycznego i administracyjnego. 3. Przedmiotem zamówienia jest **jednorazowy zakup i wdrożenie** kompletnego środowiska szkoleniowego online. 4. Na przedmiot dostawy składa się:    1. Uruchomienie dedykowanej platformy e-learningowej wraz z **opłaconym z góry dostępem** (licencjami) na okres **36 miesięcy**.    2. Dostarczenie (wytworzenie) dedykowanego wsadu merytorycznego (kursów). 5. **Model Płatności:** Wynagrodzenie za ten element ma charakter ryczałtowy (jednorazowy) i obejmuje całość kosztów związanych z utrzymaniem infrastruktury, aktualizacjami platformy oraz dostępnością usługi przez 3 lata. Płatność następuje po podpisaniu Protokołu Odbioru Wdrożenia Platformy.   **Szczegółowy Zakres Prac**  Przedmiot zamówienia obejmuje kompleksowe świadczenie usługi szkoleniowej w formie e-learningu, na które składają się dwa główne zadania:  **Zadanie 1: Dostarczenie i Utrzymanie Platformy E-learningowej**   1. **Licencja i Dostęp:** Wykonawca zapewni dostęp do platformy szkoleniowej online dla **liczby użytkowników wskazanych w zamówieniu podstawowym i prawie opcji**. Dostęp do platformy musi być gwarantowany przez okres **minimum 36 miesięcy** od daty protokolarnego odbioru przedmiotu zamówienia. 2. **Wymagania Techniczne Platformy:**    * **Dostępność:** Platforma musi być dostępna w trybie 24/7 (SLA 99,5%). Wykonawca w ramach ceny ryczałtowej udziela gwarancji utrzymania tej dostępności przez cały okres 3 lat.    * **Kompatybilność:** Platforma musi poprawnie funkcjonować na najnowszych, stabilnych wersjach popularnych przeglądarek internetowych: Google Chrome, Apple Safari, Microsoft Edge, na systemach operacyjnych Windows oraz macOS.    * **Zarządzanie Użytkownikami:** System musi umożliwiać rejestrację uczestników na podstawie adresów e-mail pochodzących z domen wskazanych przez Zamawiającego. Zamawiający przekaże Wykonawcy listę domen uprawnionych do rejestracji. 3. **Wymagania Funkcjonalne Platformy:**    * **Automatyzacja i Monitoring:** Platforma musi zapewniać:      + Automatyczne śledzenie postępów każdego uczestnika w czasie rzeczywistym.      + Możliwość wysyłania automatycznych przypomnień e-mail do uczestników, którzy nie rozpoczęli lub nie ukończyli kursu.      + Panel administracyjny dla Zamawiającego, umożliwiający generowanie w czasie rzeczywistym raportów i list osób, które ukończyły lub nie ukończyły szkolenia.      + Automatyczne generowanie imiennych certyfikatów ukończenia szkolenia (w formacie PDF) z możliwością ich samodzielnego pobrania przez uczestnika po zdaniu egzaminu końcowego.    * **Moduł Egzaminacyjny:** Kurs musi kończyć się modułem egzaminacyjnym (testem wiedzy), który weryfikuje przyswojenie materiału.   **Zadanie 2: Opracowanie i Udostępnienie Dedykowanych Kursów Szkoleniowych**  Na platformie, o której mowa w Zadaniu 1, Wykonawca udostępni kurs e-learningowy, którego treść zostanie opracowana w uzgodnieniu z Zamawiającym. Minimalny zakres merytoryczny kursu musi obejmować następujące moduły:   1. **Moduł 1: Cyberbezpieczeństwo w Ochronie Zdrowia – Fundamenty**    * **Wprowadzenie:** Dlaczego bezpieczeństwo informacji w szpitalu jest krytyczne? (Przykłady realnych incydentów w sektorze zdrowia, konsekwencje dla pacjentów i placówki).    * **Identyfikacja Zagrożeń:** Phishing (jak rozpoznawać fałszywe maile i SMSy), złośliwe oprogramowanie (wirusy, ransomware), inżynieria społeczna (jak nie dać się zmanipulować).    * **Higiena Haseł:** Zasady tworzenia silnych haseł, znaczenie uwierzytelniania wieloskładnikowego (MFA).    * **Bezpieczna Praca w Sieci:** Bezpieczne korzystanie z poczty e-mail i internetu, rozpoznawanie niebezpiecznych załączników i linków.    * **Ochrona Urządzeń:** Zabezpieczanie urządzeń mobilnych i nośników danych (pendrive, dyski zewnętrzne).    * **Bezpieczeństwo Fizyczne:** Polityka czystego biurka, ochrona wydruków zawierających dane wrażliwe. 2. **Moduł 2: System Zarządzania Bezpieczeństwem Informacji (SZBI) w Naszym Szpitalu**    * **Czym jest SZBI?** Rola i cel wdrożonego systemu w kontekście ISO 27001, KRI i RODO.    * **Moja Rola w Systemie:** Kluczowe obowiązki i odpowiedzialność każdego pracownika za bezpieczeństwo informacji.    * **Klasyfikacja Informacji:** Jak postępować z różnymi typami danych? (dane medyczne pacjentów, dane pracownicze, informacje publiczne).    * **Zgłaszanie Incydentów:** Procedura postępowania w przypadku podejrzenia incydentu bezpieczeństwa (do kogo i jak zgłosić, jakie informacje przekazać).    * **Konsekwencje Niestosowania Zasad:** Odpowiedzialność prawna i dyscyplinarna. 3. **Moduł 3: Egzamin Końcowy**    * Test wiedzy w formie jednokrotnego wyboru, składający się z minimum 20 pytań losowanych z puli.    * Warunkiem zaliczenia jest uzyskanie progu co najmniej 70% poprawnych odpowiedzi. Użytkownik ma prawo do 5 prób zaliczenia testu.   **Kluczowe Wymagania i Warunki Realizacji**   1. **Odbiór prac:** Odbiór przedmiotu zamówienia nastąpi na podstawie protokołu zdawczo-odbiorczego, podpisanego bez uwag przez obie strony, po weryfikacji przez Zamawiającego, że platforma e-learningowa została uruchomiona, jest w pełni funkcjonalna, zawiera kursy o wymaganym zakresie merytorycznym, a wskazani przedstawiciele Zamawiającego otrzymali dostęp do panelu administracyjnego. 2. **Współpraca:** Zamawiający zobowiązuje się do aktywnej współpracy z Wykonawcą, w szczególności do przekazania listy domen e-mail uprawnionych do rejestracji na platformie. 3. **Dostępność Cyfrowa:**    1. Zamawiający wymaga, aby wszystkie dokumenty przeznaczone dla użytkownika, dotyczące obsługi wdrażanych systemów tj. instrukcje, regulaminy, filmy instruktażowe, itp. spełniały standard cyfrowy opisany w załączniku nr 2 Standardy dostępności dla polityki spójności 2021-2027do Wytycznych dotyczących realizacji zasad równościowych w ramach funduszy unijnych na lata 2021–2027 (Źródło: https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/fundusze-na-lata-2021-2027/prawo-i-dokumenty/wytyczne/wytyczne-dotyczace-realizacji-zasad-rownosciowych-w-ramach-funduszy-unijnych-na-lata-2021-2027/)    2. Zamawiający wymaga, aby platforma szkoleniowa dostarczona w ramach zamówienia spełniała wymogi dostępności co najmniej w zakresie: zmiany rozmiaru czcionki, zmiany kontrastu. Zamawiający dopuszcza realizację tych funkcjonalności z wykorzystaniem funkcji sytemu operacyjnego. 4. Wykonawca zobowiązany jest do realizacji zamówienia zgodnie z zasadą "nie czyń poważnych szkód" (DNSH - Do No Significant Harm). 5. **Produkty:**  * Protokół potwierdzający udzielenie dostępu do w pełni funkcjonalnej platformy e-learningowej. * Dostęp do panelu administracyjnego platformy dla wskazanych osób po stronie Zamawiającego. |

# Prawo opcji

|  |  |  |
| --- | --- | --- |
| **Lp.** | **Wymaganie** | **Opis** |
|  | **Postanowienia Ogólne** | * 1. Zamawiający, zgodnie z postanowieniami Zapytania Ofertowego oraz Umowy, przewiduje możliwość skorzystania z Prawa Opcji.   2. Prawo Opcji stanowi jednostronne uprawnienie Zamawiającego, z którego może on skorzystać, ale nie musi. Nieskorzystanie przez Zamawiającego z całości lub części Prawa Opcji nie stanowi podstawy do jakichkolwiek roszczeń ze strony Wykonawcy.   3. Zamawiający zastrzega sobie prawo do skorzystania z Prawa Opcji w całości lub w częściach, w terminie do **6 miesięcy** od daty zawarcia umowy.   4. Uruchomienie Prawa Opcji nastąpi poprzez złożenie przez Zamawiającego pisemnego (lub w formie elektronicznej pod rygorem nieważności) oświadczenia woli o skorzystaniu z opcji, wskazującego wybrany Element, lokalizację oraz jego zakres (wolumen).   5. Ceny jednostkowe lub ryczałtowe dla poszczególnych Elementów Prawa Opcji muszą być tożsame z cenami wskazanymi przez Wykonawcę w Formularzu Ofertowym.   Zakres Prawa Opcji  W ramach Prawa Opcji Zamawiający przewiduje możliwość zamówienia następujących, dodatkowych usług i świadczeń, podzielonych na 5 Elementów: |
|  | **Element 1 Opcji: Rozszerzenie Usługi SOC oraz Systemu EDR dla jednostek powiązanych** | 1. Zamawiający przewiduje możliwość rozszerzenia świadczenia Usługi SOC (opisanej w Części 2 OPZ) oraz objęcia licencjami i ochroną Systemu EDR (opisanego w Części 2 OPZ) dla następujących, powiązanych jednostek organizacyjnych:    1. Oddział w Krakowie    2. Oddział w Warszawie    3. Oddział we Wrocławiu    4. Centrala BCM 2. W celu zapewnienia przejrzystości postępowania, Zamawiający określa maksymalny, łączny wolumen (zakres) Prawa Opcji dla każdej z ww. jednostek:    1. **Oddział w Krakowie:** maksymalnie 30 serwerów oraz 250 stacji roboczych.    2. **Oddział w Warszawie:** maksymalnie 15 serwerów oraz 55 stacji roboczych.    3. **Oddział we Wrocławiu:** maksymalnie 25 serwerów oraz 150 stacji roboczych.    4. **Centrala BCM:** maksymalnie 15 stacji roboczych. 3. Rozliczenie nastąpi na podstawie ceny jednostkowej za 1 punkt końcowy (endpoint) objęty Usługą SOC oraz licencją EDR, wynikającej z Formularza Ofertowego. |
|  | **Element 2 Opcji: Dodatkowe szkolenia z zakresu SZBI dla kadry zarządzającej** | 1. Zamawiający przewiduje możliwość zlecenia przeprowadzenia dodatkowego, dedykowanego szkolenia stacjonarnego z zakresu SZBI, o zakresie merytorycznym i organizacyjnym analogicznym do szkolenia dla kadry zarządzającej opisanego w Części 3 OPZ. 2. Łączna maksymalna liczba osób do przeszkolenia w ramach opcji wynosi:    1. **Oddział w Krakowie:** 26 osób (1 grupa szkoleniowe).    2. **Oddział w Warszawie:** 27 osób (1 grupa szkoleniowe).    3. **Oddział we Wrocławiu:** 18 osób (1 grupa szkoleniowa).    4. **Centrala BCM:** 11 osób (1 grupa szkoleniowa). 3. Rozliczenie nastąpi na podstawie ceny jednostkowej za realizację 1 szkolenia (dla grupy do 18 osób), wynikającej z Formularza Ofertowego. |
|  | **Element 3 Opcji: Rozszerzenie dostępu do platformy e-learningowej** | 1. Zamawiający przewiduje możliwość dokupienia dostępu do platformy e-learningowej (opisanej w Części 3 OPZ) dla dodatkowych użytkowników. 2. Maksymalny, łączny zakres (wolumen) Prawa Opcji dla tego Elementu ustala się na **1300 dodatkowych użytkowników**, z podziałem na alokację:    1. **Oddział w Krakowie:** do 500 użytkowników.    2. **Oddział w Warszawie:** do 600 użytkowników.    3. **Oddział we Wrocławiu:** do 160 użytkowników.    4. **Centrala BCM:** do 40 użytkowników.   Rozliczenie nastąpi na podstawie ceny jednostkowej za udzielenie dostępu dla 1 dodatkowego użytkownika, wynikającej z Formularza Ofertowego |
|  | **Element 4 Opcji: Wdrożenie SZBI w Jednostkach Powiązanych** | 1. Zamawiający przewiduje możliwość zlecenia realizacji prac wdrożeniowych Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach powiązanych wymienionych w Elemencie 1. 2. Dla każdej wskazanej przez Zamawiającego jednostki, zakres prac jest analogiczny do Etapów I-IV zamówienia podstawowego i obejmuje: 3. Przeprowadzenie lokalnego Audytu Zerowego i analizy luk. 4. Przeprowadzenie szacowania ryzyka uwzględniającego specyfikę lokalną oddziału. 5. Adaptację i wdrożenie dokumentacji SZBI (w tym polityk i procedur) dla danej lokalizacji. 6. Przeprowadzenie szkoleń wdrożeniowych dla personelu w danej lokalizacji.   Rozliczenie nastąpi na podstawie ceny ryczałtowej za pełne wdrożenie w jednej lokalizacji, wynikającej z Formularza Ofertowego. |
|  | **Element 5 Opcji: Usługa Nadzoru (Security Officer) w Jednostkach Powiązanych** | 1. Zamawiający przewiduje możliwość rozszerzenia świadczenia usługi ciągłego nadzoru nad utrzymaniem SZBI (funkcja "Security Officer") na jednostki powiązane (wymienione w Elemencie 1), w odniesieniu do których Zamawiający skorzystał z Prawa Opcji w zakresie Elementu 1 (SOC/EDR) lub Elementu 4 (Wdrożenie SZBI). 2. Zakres usługi jest tożsamy z opisem "Usługi Nadzoru nad Utrzymaniem SZBI" w zamówieniu podstawowym i obejmuje dla każdej wskazanej lokalizacji: 3. Monitorowanie zgodności lokalnych procesów z dokumentacją SZBI. 4. Realizację cyklicznych przeglądów bezpieczeństwa w danej lokalizacji. 5. Aktualizację dokumentacji w odpowiedzi na zmiany specyficzne dla danego oddziału. 6. Wsparcie lokalnego personelu w obsłudze incydentów i wyjaśnieniach. 7. Usługa będzie świadczona w okresie obowiązywania umowy, od momentu złożenia oświadczenia o uruchomieniu opcji do końca trwania umowy głównej. 8. Rozliczenie nastąpi na podstawie miesięcznej stawki ryczałtowej za świadczenie usługi nadzoru dla jednej lokalizacji, wynikającej z Formularza Ofertowego. |