I. Przedmiot zamówienia

Przedmiotem zamówienia jest:

1) Dostawa licencji oprogramowania dla systemu SIEM wraz z modułem SOAR.
2) Wdrożenie i konfiguracja systemu SIEM.
3) Dostawa, wdrożenie i konfiguracja darmowego skanera podatności open source.
4) Wdrożenie i konfiguracja modułu SOAR.
5) Przygotowanie i dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej, dokumentacji dla użytkownika, dokumentacji powdrożeniowej.
6) Szkolenie/warsztaty z obsługi SIEM i SOAR.
7) Zapewnienia 24-miesięcznej gwarancji dla systemu SIEM, SOAR i skanera podatności.
8) Zapewnienie usługi wsparcia technicznego dla systemu SIEM, SOAR i skanera podatności, w maksymalnej liczbie 300 godzin roboczych.

Opis Przedmiotu Zamówienia zawiera minimalne wymagania jakie musi spełnić Wykonawca na potrzeby realizacji przedmiotu zamówienia.

II. Opis infrastruktury Zamawiającego

Opis zostanie uzupełniony po wstępnych konsultacjach rynkowych.

III. Słownik pojęć i skrótów

Termin	Definicja
Administrator systemu	Rola w systemie SIEM odpowiedzialna za konfigurację i bieżący nadzór nad prawidłowym działaniem systemu, posiadająca uprawnienia do akceptacji kluczowych operacji w systemie.
Błąd Krytyczny/Awaria	Oznacza brak działania środowiska produkcyjnego systemu SIEM, praca nie może być kontynuowana, operacja krytyczna dla procesu biznesowego jest niemożliwa. Błąd Krytyczny ma jedną lub więcej z poniższych cech: 1. Dane biznesowe zostały uszkodzone. 2. Funkcjonalność krytyczna systemu SIEM nie działa. 3. System w zakresie Funkcjonalności krytycznych przerywa działania i nie daje się uruchomić pomimo prób, stosując procedury przygotowane przez Wykonawcę lub procedury przygotowane przez Zamawiającego i zaakceptowane przez Wykonawcę w trakcie okresu Gwarancji. 4. Wszelkie błędy związane z bezpieczeństwem przechowywania i przetwarzania danych, które mogą wpłynąć na: a) uwierzytelnianie, b) niezaprzeczalność, c) poufność, d) integralność, e) dostępność, f) rozliczalność. 5. Wszelkie awarie związane z bezpieczeństwem dostępu do systemu

Termin	Definicja
	SIEM (w tym nieautoryzowanym dostępem do danych). Błąd Krytyczny/Awaria wymaga reakcji i naprawy z zachowaniem zdefiniowanego SLA.
Błąd Drobny/Usterka	Błąd uniemożliwiający wykonanie pewnego zadania, błędne działanie systemu SIEM, błąd, dla którego możliwe jest zastosowanie przebiegu alternatywnego: 1. Błędne działanie systemu SIEM. 2. Dotyczy funkcjonalności, która jest rzadziej używana. 3. Problemy niemające wpływu na ciągłość procesów biznesowych, powodujące uciążliwości w pracy systemu. 4. Błędy wydajnościowe, które zwalniają działanie systemu, ale nie blokują jego działania. Błąd Drobny/Usterka wymaga reakcji i naprawy z zachowaniem zdefiniowanego SLA.
Czas Naprawy	Czas liczony od momentu potwierdzenia przez Wykonawcę przyjęcia Zgłoszenia do momentu dostarczenia poprawki naprawiającej Błąd Krytyczny/Awarię lub Błąd Drobny/Usterkę lub wdrożenia Obejścia dla Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki. W przypadku dostarczenia poprawki lub wdrożenia Obejścia, które nie usuwają Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki Czas Naprawy uważa się za niedochowany.
Czas Obejścia	Czas liczony od momentu skutecznego wdrożenia przez Wykonawcę Obejścia do momentu dostarczenia poprawki naprawiającej Błąd Krytyczny/Awarię lub Błąd Drobny/Usterkę.
Czas Reakcji	Czas liczony od momentu przekazania przez Zamawiającego Zgłoszenia o Błędzie Krytycznym/Awarii lub Błędzie Drobnym/Usterce do momentu potwierdzenia przez Wykonawcę przyjęcia Zgłoszenia.
Dzień Roboczy	Dzień od poniedziałku do piątku, z wyjątkiem dni ustawowo wolnych od pracy w Polsce, w godz. 8:00 – 18:00.
Dokumentacja	Wszelka dokumentacja dotycząca wdrażanego rozwiązania lub jakichkolwiek innych prac Wykonawcy, która jest dostarczana lub powstanie w ramach realizacji przedmiotu zamówienia, w tym np. dokumentacja analityczna, testowa, powykonawcza i eksploatacyjna.
Funkcjonalność krytyczna	Funkcjonalność systemu SIEM istotna z punktu widzenia bezpieczeństwa oraz zachowania ciągłości działania systemu.
Korelacja / korelacja zdarzeń	Przez korelację zdarzeń rozumie się automatyczne, realizowane na bieżąco wyszukiwanie zależności między różnymi zdarzeniami z wielu źródeł, agregację i wzbogacanie danych. Korelacja odbywa się na podstawie zdefiniowanych reguł określających te zależności.
Niestandardowe źródło danych	Jest to źródło danych, dla którego system SIEM nie posiada gotowego mechanizmu integracji (parsera) lub wymaga on dostosowania do specyfiki źródła danych.
Oprogramowanie standardowe	Oprogramowanie towarzyszące i niezbędne do funkcjonowania systemu będącego przedmiotem zamówienia, takie jak systemy operacyjne, wirtualizatory, systemy baz danych, systemy kopii zapasowych, systemy monitorowania, sterowniki itp.

Termin	Definicja
Oprogramowanie dedykowane	Oprogramowanie będące przedmiotem zamówienia: System SIEM wraz z modułem SOAR oraz skanerem podatności.
System SIEM	(Security Information Event Management) system klasy SIEM, do którego głównych zadań należy gromadzenie i korelacja zdarzeń przesyłanych lub pobieranych z innych systemów.
Wdrożenie	Doprowadzenie do uzyskania pełnej wymaganej przez Zamawiającego funkcjonalności systemu SIEM, SOAR, skanera podatności
Wykonawca	Podmiot realizujący przedmiot zamówienia, wyłoniony w wyniku niniejszego postepowania zamówień publicznych.
Zamawiający	Główny Inspektorat Sanitarny.
Zasób / Zasób IT	Elementy infrastruktury IT, z których system SIEM pozyskuje dane o zdarzeniach systemowych np. serwery (fizyczne i wirtualne), stacje robocze, urządzenia sieciowe, systemy teleinformatyczne, bazy danych, pliki itp.
Zlecenie	Zlecenie składane przez Zamawiającego na realizację określonych prac dodatkowych w ramach usługi wsparcia.
Zgłoszenie	Informacja przekazana Wykonawcy przez administratora systemu o Błędzie Krytycznym/Awarii, Błędzie Drobnym/Usterce lub Zleceniu.
Źródła zdarzeń	Elementy infrastruktury IT, z których system SIEM wraz z modułem SOAR pozyskuje dane o zdarzeniach systemowych np. serwery (fizyczne i wirtualne), stacje robocze, urządzenia sieciowe, systemy teleinformatyczne, bazy danych, pliki itp.

IV. Wymagania dla rozwiązania SIEM + SOAR

Identyfikator	Opis wymagania
WR.1	Dostarczone rozwiązanie musi być systemem klasy SIEM (Security Information Event Management), którego celem jest gromadzenie i korelacja zdarzeń systemowych (w tym zdarzeń bezpieczeństwa), przesyłanych lub pobieranych z innych systemów i urządzeń teleinformatycznych.
WR.2	System SIEM musi być wyposażony w moduł obsługi incydentów SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń.
WR.3	System SIEM i SOAR muszą być jednym zintegrowanym rozwiązaniem klasy enterprise, jednego producenta wraz z jego wsparciem. Nie dopuszcza się rozwiązań darmowych/open source oraz rozwiązań składających się z wielu osobnych modułów różnych producentów.
WR.4	System SIEM musi pracować zachowując pełną funkcjonalność w modelu on premises w wyizolowanej infrastrukturze Zamawiającego. Zamawiający nie dopuszcza rozwiązań w modelu chmurowym.
WR.5	System SIEM i SOAR musi umożliwiać instalację w wirtualnym środowisku VMware vSphere posiadanym przez Zamawiającego.

Identyfikator	Opis wymagania
WR.6	Wszystkie komponenty wchodzące w skład Systemu SIEM i modułu SOAR muszą być w wersji produkcyjnej. Nie dopuszcza się komponentów w wersjach beta.
WR.7	Wykonawca dostarczy najnowsze wersje oprogramowania dla elementów Systemu SIEM oraz modułu SOAR na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez producenta rozwiązania.
WR.8	System SIEM i SOAR muszą umożliwić, autoryzację użytkowników oraz precyzyjne nadawanie uprawnień dla administratorów i użytkowników oraz zapewniać pełną ich rozliczalność, a także zapewniać poufność transmisji danych.
WR.9	System SIEM i SOAR muszą posiadać graficzny interfejs użytkownika, możliwy do uruchomienia przez nowoczesną przeglądarkę internetową (Chrome, Edge, Firefox, Safari, Opera), bez konieczności instalowania dodatków do przeglądarki oraz innego dodatkowego oprogramowania. Nie dopuszcza się rozwiązań wymuszających wykorzystywanie niewspieranych przeglądarek i dodatków.
WR.10	System SIEM musi gwarantować możliwość elastycznej rozbudowy o dalsze zasoby IT, które w przyszłości zostaną objęte jego działaniem.
WR.11	System SIEM i SOAR muszą umożliwiać równoczesną pracę 5 operatorów oraz objąć monitoringiem200 zasobów IT.
WR.12	System SIEM musi umożliwiać przetwarzanie zdarzeń w ilości 30 000 zdarzeń na sekundę.
WR.13	Wszelkie dostarczone oprogramowania muszą posiadać licencje wieczyste. Zamawiający nie dopuszcza subskrypcji.
WR.14	System SIEM musi przechowywać zgromadzone dane w wysokiej dostępności przez okres min. 90 dni oraz zapewniać automatyczną archiwizację po upływie tego terminu.
WR.15	Wykonawca dostarczy, uruchomi i zintegruje z systemem SIEM darmowy skaner podatności open source.

V. Wymagania funkcjonalne systemu SIEM + SOAR

Identyfikator	Opis wymagania
WFU.1	System SIEM musi zapewniać odbiór lub pobieranie danych za pośrednictwem protokołów SYSLOG oraz NetFlow, mechanizmu Windows Event Forwarding (WEF) oraz sterownika ODBC.
WFU.2	System SIEM umożliwiać automatyczne pobieranie logów audytowych systemów baz danych.
WFU.3	System SIEM musi być wyposażony w mechanizmy normalizacji (parsowania) pozyskanych danych przez ich podział na pola, na podstawie których może odbywać się dalsze przetwarzanie oraz wyszukiwanie danych.
WFU.4	Proces normalizacji (parsowania) systemu SIEM musi odbywać się na bieżąco na etapie rejestrowania danych w systemie.
WFU.5	Normalizacja systemu SIEM musi uwzględniać możliwość nadawania kategorii zdarzeń na podstawie wartości parsowanych pól.

Identyfikator	Opis wymagania
WFU.6	System SIEM musi posiadać predefiniowany zestaw reguł normalizacji (parsowania) logów dla popularnych źródeł logów takich jak: urządzenia sieciowe, systemy bezpieczeństwa, systemy Windows i Linux, Active Directory.
WFU.7	System SIEM musi być wyposażony w mechanizmy reguł opartych na mechanizmach behawioralnych z możliwością agregacji danych oraz punktowania poszczególnych zdarzeń w wyznaczonych oknach czasowych. W rezultacie działania reguł behawioralnych system musi tworzyć incydenty związane z przekroczeniem dozwolonych zakresów punktacji dla zdarzeń zaobserwowanych w oknie czasowym agregacji.
WFU.8	System SIEM musi umożliwiać budowanie profili aktywności użytkowników oraz zasobów IT poprzez wielowartościowe listy referencyjne i wykorzystywać je w regułach korelacyjnych.
WFU.9	System SIEM musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) logów z niestandardowych źródeł danych, w oparciu o składnię wyrażeń regularnych, JSON lub XML. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia.
WFU.10	System SIEM musi rejestrować i przechowywać pozyskane dane w wersji pierwotnej oraz w wersji znormalizowanej.
WFU.11	System SIEM musi umożliwiać automatyczną archiwizację danych na zewnętrzne repozytoria danych.
WFU.12	System SIEM musi być wyposażony w graficzny interfejs umożliwiający przeglądanie i przeszukiwanie zarejestrowanych danych w formie znormalizowanej i pierwotnej.
WFU.13	System SIEM musi prezentować wyniki wyszukiwania z zastosowaniem filtrów opartych na wartościach pól, złożonych wyrażeniach logicznych, wskazaniach zakresu czasowego i źródła danych.
WFU.14	Interfejs wyszukiwania systemu SIEM musi umożliwiać zapisywanie zapytań z możliwością ich ponownego wykorzystania w przyszłości.
WFU.15	System SIEM musi zawierać narzędzia do zautomatyzowanego tworzenia elektronicznej, interaktywnej dokumentacji infrastruktury teleinformatycznej uwzględniając schematy architektury zabezpieczeń sieci tzn. mapy pokazującej urządzenia zabezpieczeń, strefy bezpieczeństwa, zasoby teleinformatyczne, połączenia i topologię sieci LAN/WAN), prezentującej informacje nt. bezpieczeństwa w ujęciu technicznym oraz w odniesieniu do procesów działania organizacji.
WFU.16	System SIEM musi być wyposażony w mechanizmy zautomatyzowanego, dynamicznego uzupełniania elektronicznej dokumentacji na podstawie danych pozyskanych z logów i informacji o ruchu sieciowym (Netflow), protokołów SNMP, WMI, SSH, skanerów podatności oraz skryptów PowerShell za pomocą których musi istnieć możliwość precyzyjnego określenia zakresu danych, które mają zostać uzupełnione. System musi posiadać repozytorium gotowych skryptów oraz graficzny interfejs pozwalający na tworzenie nowych skryptów, obejmujący możliwość przekazywania do nich parametrów wejściowych.

Identyfikator	Opis wymagania
WFU.17	Mechanizmy automatycznego uzupełniania dokumentacji elektronicznej muszą uwzględniać informacje o typach zasobów (np. serwer WWW, baza danych, serwer plików, stacja robocza) oraz zależnościach między tymi zasobami (np.: stacja robocza łączy się do serwera baz danych).
WFU.18	Elektroniczna dokumentacja infrastruktury teleinformatycznej systemu SIEM musi pozwalać na wprowadzenie informacji o procesach biznesowych oraz technicznych oraz określania powiązań procesów z elementami infrastruktury (np.: serwer X związany jest z procesami A i B).
WFU.19	Informacje o procesach biznesowych muszą uwzględniać ważność procesów dla organizacji, typy danych przetwarzanych w ramach procesów (np. dane osobowe, informacje poufne itp.), właścicieli procesów, relacje między procesami (np. proces A zależy od procesu B, przy czym zależności powinny być prezentowane w formie graficznej) oraz czas trwania procesów (np. proces praca biurowa w organizacji jest aktywny od poniedziałku do piątku od 8:00 do 16:00).
WFU.20	Interfejs systemu elektronicznej dokumentacji systemu SIEM musi umożliwiać wizualizację informacji o infrastrukturze teleinformatycznej.
WFU.21	Wizualizacja musi obejmować interaktywną mapę logiczną sieci z zaznaczonymi strefami sieci, strefami bezpieczeństwa, urządzeniami sieciowymi, połączeniami, systemami zabezpieczeń IT oraz procesami.
WFU.22	Interfejs interaktywnej mapy sieci musi umożliwiać wyświetlanie i modyfikowanie szczegółowych informacji o każdym elemencie infrastruktury IT oraz posiadać mechanizm definiowania dozwolonej komunikacji sieciowej dla każdego zasobu IT, który został zdefiniowany w elektronicznej dokumentacji.
WFU.23	System musi pozwalać na definiowanie własnych parametrów dla wszystkich typów obiektów zgromadzonych w elektronicznej dokumentacji sieci.
WFU.24	System SIEM musi umożliwiać prezentację danych zgromadzonych w elektronicznej dokumentacji infrastruktury IT również w formie tabelarycznej.
WFU.25	Interfejs systemu SIEM musi pozwalać na manualne zmiany wartości parametrów obiektów, dodawanie obiektów oraz ich usuwanie, bezpośrednio z poziomu widoku mapy oraz tabeli.
WFU.26	System SIEM musi prezentować techniczne informacje nt. bezpieczeństwa IT z perspektywy działalności organizacji, w tym zapisywanie, wyszukiwanie i prezentowanie co najmniej następujących informacji: procesy biznesowe organizacji oraz wspierające je procesy techniczne i powiązane z nimi zasoby IT, klasyfikacja zbiorów informacji przetwarzanych w ramach wskazanych procesów oraz przez wskazane zasoby IT, ważność zasobów IT dla organizacji ze względu na typ przetwarzanych danych oraz wspierane procesy, właścicieli zasobów (Owners) oraz zespół IT odpowiedzialny za jego obsługę (Custodians).
WFU.27	System SIEM musi umożliwiać wykrywanie topologii sieci fizycznej oraz jej wizualizacji na podstawie następujących protokołów sieciowych: SNMP v2 i v3, LLDP, CDP.

Identyfikator	Opis wymagania
WFU.28	System elektronicznej dokumentacji systemu SIEM musi zawierać bazę wiedzy eksperckiej uwzględniającej wiedzę, która pozwoli ocenić poprawność projektu zabezpieczeń, identyfikując efektywność zastosowanych mechanizmów sieciowych oraz lokalnych w stosunku do potencjalnych wektorów ataków oraz w przypadku ich niezastosowania zidentyfikować ryzyka, które się z tym wiążą.
WFU.29	Interfejs elektronicznej dokumentacji systemu SIEM musi umożliwiać automatyczne wyszukiwanie pojedynczych, potencjalnych punktów awarii sieci i systemów IT, których uszkodzenie może spowodować zablokowanie ważnych procesów organizacji.
WFU.30	System SIEM dla zarejestrowanych zdarzeń/ incydentów, musi automatycznie wyznaczać ścieżkę ataku i zaprezentować ją w formie graficznej na schemacie sieci organizacji. Ścieżka ataku pokazuje wszystkie urządzenia zabezpieczeń na drodze pomiędzy celem a źródłem zdarzenia lub incydentu.
WFU.31	System SIEM musi pozwalać na automatyczne szacowanie ryzyka cyber zagrożeń dla wszystkich zasobów IT zdefiniowanych w elektronicznej dokumentacji infrastruktury teleinformatycznej. Szacowanie ryzyka musi uwzględniać architekturę sieci, typy zasobów informatycznych, zabezpieczenia oraz procesy i związane z nimi konsekwencje.
WFU.32	System SIEM musi zapewniać narzędzia umożliwiające dokonanie oceny wpływu incydentu bezpieczeństwa IT na działalność organizacji (np.: system wyszukuje i prezentuje informacje nt. procesów organizacji i klasyfikowanych informacji, które mogły zostać naruszone w wyniku incydentu oraz wyświetla przewidywane istotne dla organizacji konsekwencje naruszenia bezpieczeństwa).
WFU.33	System SIEM musi zawierać narzędzia służące do ustalania wrażliwych zbiorów informacji, jakie są narażone w razie incydentu bezpieczeństwa oraz narzędzia umożliwiające definiowanie własnego schematu klasyfikacji danych w organizacji (np. własność intelektualna, dane osobowe, dane finansowe) oraz zapewniać wyszukiwanie lokalizacji zasobów teleinformatycznych, gdzie znajdują się dane określonej kategorii ze wskazaniem ich na graficznej mapie systemu teleinformatycznego.
WFU.34	System SIEM musi posiadać narzędzia do modelowania zagrożeń, umożliwiając symulowanie potencjalnych scenariuszy bezpieczeństwa.

Identyfikator	Opis wymagania
WFU.35	Interfejs mapy sieci systemu SIEM musi pozwalać m.in. na: a) wyznaczenie źródła zagrożenia zasobu teleinformatycznego wraz z wynikiem analizy ryzyka dla tego zagrożenia wyliczanym w sposób automatyczny, b) wyświetlanie zabezpieczeń zasobu teleinformatycznego przed potencjalnymi źródłami zagrożenia, c) wyświetlanie zabezpieczeń chroniących zasoby teleinformatyczne przed określonym źródłem zagrożenia, d) wyświetlanie lokalizacji zasobów określonego rodzaju, e) wyświetlanie najbardziej narażonych zasobów teleinformatycznych, f) wyświetlanie ważnych zasobów teleinformatycznych narażonych na awarie.
WFU.36	System SIEM musi zapewniać graficzne narzędzia do definiowania wymagań bezpieczeństwa organizacji (m.in. środków ochrony wymaganych dla określonych elementów i obszarów systemu teleinformatycznego) oraz narzędzia do audytowania bezpieczeństwa względem tych wymagań.
WFU.37	Narzędzia systemu SIEM muszą umożliwiać m.in.: a) wyznaczanie zasobów IT o wysokim poziomie ryzyka, które nie posiadają wymaganych zabezpieczeń, b) wskazywanie zasobów IT o krytycznym znaczeniu dla organizacji, które nie posiadają odpowiednich zabezpieczeń.
WFU.38	System SIEM musi umożliwiać uwzględnianie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej w mechanizmach korelacji zdarzeń. Wykryte zdarzenia/ incydenty będą priorytetyzowane w odniesieniu do ważności dla organizacji zasobów, których dotyczą (np.: wspomaganych procesów, przetwarzanych informacji klasyfikowanych).
WFU.39	System SIEM musi umożliwiać uwzględnianie wyników szacowania ryzyka w mechanizmach korelacji zdarzeń.
WFU.40	System SIEM w razie wykrycia incydentów o poważnych konsekwencjach dla organizacji musi umożliwiać automatyczne powiadamianie o incydencie wskazanych pracowników, m.in. za pomocą email.
WFU.41	System SIEM musi pozwalać na prezentację danych w postaci tzw. „Dashboard”, tj. dostosowywać zakres i prezentacje danych do potrzeb administratora czy też zalogowanego użytkownika.
WFU.42	System SIEM musi być wyposażony w moduł obsługi incydentów SOAR (Security Orchestration, Automation And Response) raportowanych przez mechanizmy korelacji zdarzeń. Moduł obsługi incydentów może stanowić integralną część systemu SIEM lub być dostarczony w ramach odrębnego, zintegrowanego z systemem SIEM, rozwiązania tego samego producenta.
WFU.43	Moduł obsługi incydentów systemu SIEM musi wspierać proces obsługi incydentów. W ramach procesu każdy incydent musi przejść proces selekcji, analizy, oceny wpływu i reakcji. W ramach procesu każdy incydent musi przyjmować stany właściwe dla etapów procesu obsługi incydentów np.: nowe zdarzenie, incydent, fałszywy alarm, incydent zamknięty.

Identyfikator	Opis wymagania
WFU.44	Moduł obsługi incydentów musi umożliwiać przydzielanie zadań w ramach obsługi incydentu.
WFU.45	Moduł obsługi incydentów systemu SIEM musi zapewniać graficzny interfejs wspierający proces obsługi incydentów, którego zadaniem będzie wspieranie użytkownika w realizacji zadań związanych z selekcją zdarzeń, analizą incydentów, oceną wpływu i reakcją na incydenty. Do zadań tych należą między innymi: a) wzbogacanie danych kontekstowych, b) gromadzenie artefaktów danych związanych z incydentem, c) współpraca z innymi członkami zespołu, d) komunikacja w ramach zespołu, e) wykonywanie czynności związanych z reakcją na incydent, f) raportowanie przebiegu incydentu.
WFU.46	Interfejs modułu obsługi incydentów systemu SIEM musi prezentować dane na temat incydentu: a) zdarzenia związane z incydentem, b) informacje o zasobach związanych z incydentem na podstawie danych zgromadzonych w elektronicznej dokumentacji infrastruktury teleinformatycznej, c) informacje o wynikach szacowania ryzyka dla zasobów związanych z incydentem, d) informacje o zadaniach wyznaczonych w ramach obsługi incydentu, e) listę powiązanych incydentów, f) listę podatności zasobów związanych z incydentem.
WFU.47	Moduł obsługi incydentów systemu SIEM musi być wyposażony w mechanizm scenariuszy obsługi incydentów.
WFU.48	Moduł obsługi incydentów systemu SIEM musi posiadać mechanizmy automatycznego wykonania scenariuszy, elementów scenariuszy lub akcji.
WFU.49	Moduł obsługi incydentów systemu SIEM musi umożliwiać zmianę statusu incydentów na podstawie rezultatów akcji i elementów decyzyjnych scenariuszy.
WFU.50	Moduł obsługi incydentów systemu SIEM musi być wyposażony w mechanizmy automatycznego dopasowania scenariuszy do incydentów. Dopasowanie musi uwzględniać co najmniej: a) priorytet incydentu wynikający z rezultatów działania reguł korelacji zdarzeń, b) ważność zasobu związanego z incydentem ustalana automatycznie na podstawie informacji uzyskanych z modułu dokumentacji elektronicznej, c) typ zasobu, którego dotyczy incydent ustalony automatycznie na podstawie informacji pozyskanych z modułu dokumentacji elektronicznej, d) aktualny status zdarzenia bądź incydentu w procesie obsługi incydentu.
WFU.51	Moduł obsługi incydentów systemu SIEM musi rejestrować wszystkie czynności wykonane przez użytkownika w ramach realizacji scenariuszy.

Identyfikator	Opis wymagania
WFU.52	Moduł obsługi incydentów systemu SIEM musi być wyposażony w graficzny interfejs umożliwiający tworzenie i testowanie scenariuszy obsługi incydentów.
WFU.53	System SIEM musi umożliwiać dokonanie zautomatyzowanej oceny wpływu incydentu bezpieczeństwa IT zidentyfikowanego przez mechanizmy korelacji SIEM na procesy określone w module elektronicznej dokumentacji infrastruktury teleinformatycznej.
WFU.54	Moduł obsługi incydentów systemu SIEM musi umożliwiać ustalanie przewidzianych czasów reakcji i czasów obsługi dla incydentów ze względu na ich priorytet. System musi dokonywać automatycznego pomiaru czasów reakcji na incydenty oraz czasów obsługi incydentów. Wyniki pomiaru czasu powinny być stale aktualizowane i prezentowane w interfejsie systemu.
WFU.55	Moduł obsługi incydentów systemu SIEM musi być wyposażony w mechanizm automatycznego powiadamiania wskazanych adresatów o nowych incydentach, zmianach statusów incydentów, przekroczeniach czasów reakcji i obsługi.
WFU.56	System SIEM musi być wyposażony w graficzny interfejs prezentujący w formie wykresów dane statystyczne związane z procesem obsługi incydentów. Wykresy muszą umożliwiać prezentację danych uwzględniających co najmniej: a) ilość incydentów w czasie, w podziale na priorytety, b) czasy reakcji i obsługi, c) ilości incydentów obsługiwanych przez poszczególnych użytkowników.
WFU.57	System SIEM musi umożliwiać korelację zdarzeń pochodzących z różnych urządzeń, punktów końcowych i aplikacji z anomaliami wykrywanymi w przepływach sieciowych oraz podatności pozyskanych bezpośrednio ze skanerów aplikacyjnych i bazy CVE.
WFU.58	System SIEM musi zawierać mechanizm integracji ze skanerami podatności co najmniej dwóch producentów oraz co najmniej jednym skanerem podatności dostępnym na zasadach open source. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności i importowania jego wyników.
WFU.59	Mechanizmy modułu dokumentacji elektronicznej systemu SIEM muszą umożliwiać powiązanie danych o zasobach z informacjami pozyskanymi w rezultacie skanowania podatności.

Identyfikator	Opis wymagania
WFU.60	Moduł obsługi incydentów bezpieczeństwa systemu SIEM musi umożliwiać obsługę wykrytych podatności na zasadach zbliżonych do obsługi incydentów. Zasady te dotyczą w szczególności: a) scenariuszy obsługi wraz z elementami decyzyjnymi i akcjami, b) określenie statusu w ramach procesu obsługi (np.: nowa podatność, potwierdzona podatność, wymagana aktualizacja, akceptacja podatności itp.), c) automatyczne ustalanie priorytetów podatności, d) automatyczne mierzenie czasów reakcji i obsługi, e) automatyczne powiadamianie (np.; przy pomocy email lub SMS), f) automatyczne przydzielanie zespołu obsługi do podatności, g) tworzenie i śledzenie zadań.
WFU.61	System SIEM musi zawierać mechanizm definiowania harmonogramów skanowania podatności oraz na ich podstawie automatycznie uruchamianie procesów skanowania i analizowania uzyskanych raportów.
WFU.62	System SIEM w formie graficznej musi prezentować podsumowanie aktualnego stanu bezpieczeństwa, m.in. procesy organizacji zagrożone przez incydenty oraz podatności, średni czas obsługi incydentu lub podatności.
WFU.63	System SIEM musi zapewniać możliwość rozbudowy w przyszłości o dodatkowe moduły funkcjonalne.
WFU.64	Wykonawca dostarczy mechanizm (w postaci skryptu, bądź innego rozwiązania programowego) do archiwizacji całości systemu umożliwiającego odtworzenie kompletnego systemu.

VI. Wymagania dotyczące wdrożenia

Proces wdrożeniowy systemu SIEM, SOAR wraz ze skanerem podatności podzielony zostanie na 2 Etapy:

Etap 1

Identyfikator	Opis wymagania
WWDRE1.01	Wykonawca zapewni współpracę z Zamawiającym w zakresie m.in. wprowadzenia do metodyki oraz uzupełnienia ankiety przedwdrożeniowej systemu SIEM.
WWDRE1.02	Wdrożenie systemu SIEM musi zostać wykonane we wskazanej przez Zamawiającego lokalizacji (na terenie miasta Warszawa).
WWDRE1.03	Wykonawca przedstawi projekt wdrożenia systemu SIEM w infrastrukturze Zamawiającego.
WWDRE1.04	Wykonawca dostarczy licencję na oprogramowanie systemu SIEM i SOAR.

Identyfikator	Opis wymagania
WWDRE1.05	Wykonawca uruchomi system SIEM w infrastrukturze Zamawiającego, w tym: a) przeprowadzi konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu SIEM, b) zainstaluje i skonfiguruje niezbędne oprogramowanie standardowe oraz serwery wirtualne, c) zainstaluje system SIEM, d) zestawi połączenia zdalnego dostępu, e) aktywuje licencje, f) wykona konfigurację systemu SIEM.
WWDRE1.06	Wykonawca podłączy wskazane przez Zamawiającego źródła zdarzeń.
WWDRE1.07	Wykonawca dostarczy, uruchomi i zintegruje z systemem SIEM darmowy skaner podatności open source.
WWDRE1.08	Wykonawca uruchomi i skonfiguruje parsery dla niestandardowych źródeł danych, jeżeli integracja ze wskazanymi przez Zamawiającego źródłami będzie tego wymagała.
WWDRE1.09	Wykonawca uruchomi i skonfiguruje reguły korelacyjne, elektroniczną dokumentację infrastruktury, ustawienia i obszary bezpieczeństwa infrastruktury i sieci, mechanizmy oceny ryzyka, mechanizmy powiadamiania oraz obsługi incydentów.
WWDRE1.10	Wykonawca dostroi i skalibruje reguły korelacji.
WWDRE1.11	Wykonawca dostarczy dokumentację powdrożeniową oraz dokumentację systemu SIEM (techniczną oraz dla użytkownika).
WWDRE1.12	Wykonawca zapewni transfer wiedzy w formie spotkania podsumowującego Etap 1 wdrożenia.

Etap 2

Identyfikator	Opis wymagania
WWDRE2.01	Wykonawca uruchomi system SOAR w infrastrukturze Zamawiającego, w tym: a) przeprowadzi konsultacje w przygotowaniu infrastruktury Zamawiającego do instalacji systemu SOAR, b) zainstaluje i skonfiguruje niezbędne oprogramowanie standardowe oraz serwery wirtualne, c) zainstaluje system SOAR, d) zestawi połączenia zdalnego dostępu, e) aktywuje licencje, f) wykona konfigurację systemu SOAR w tym uruchomi i skonfiguruje mechanizmy wykonywania scenariuszy automatyzacji SOAR.
WWDRE2.02	Wykonawca dostarczy dokumentację powdrożeniową oraz dokumentację systemu SOAR (techniczną oraz dla użytkownika).
WWDRE2.03	Wykonawca dokona niezbędnych integracji SOAR z innymi systemami w celu automatycznego wykonywania poleceń w ramach scenariuszy SOAR.
WWDRE2.04	Wykonawca przeprowadzi szkolenia/warsztaty dla administratorów.

Identyfikator	Opis wymagania
WWDRE2.05	Wykonawca zapewni transfer wiedzy w formie spotkania podsumowującego Etap 2 wdrożenia.

VII. Wymagania w zakresie wsparcia technicznego

Identyfikator	Opis wymagania
WAT.1	W ramach usługi wsparcia technicznego Wykonawca będzie zobowiązany do realizacji dodatkowych Zleceń, które będą wynikały z eksploatacji wdrożonych elementów przedmiotu zamówienia.
WAT.2	Całkowita liczba godzin Zleceń nie przekroczy 300 godzin roboczych.
WAT.3	W toku trwania umowy Wykonawca zapewni aplikację klasy ITSM na potrzeby rejestracji zgłoszeń Zamawiającego.
WAT.4	Zgłoszenia będą dokonywane przez Zamawiającego w trybie NBD.
WAT.5	Zgłoszenia będą obsługiwane przez Wykonawcę w ramach zdefiniowanych parametrów SLA.
WAT.6	Zgłoszenia przekazywane przez Zamawiającego będą posiadały następujące kategorie: 1) Błąd Krytyczny/Awaria. 2) Błąd Drobny/Usterka. 3) Zlecenie prac dodatkowych.
WAT.7	W ramach usługi wsparcia Wykonawca musi przeprowadzić analizę i implementację poprawek mających na celu przywrócenie funkcjonalności Systemu SIEM, SOAR lub skanera podatności w przypadku zaistnienia Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki.
WAT.8	Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie Systemu SIEM, SOAR lub skanera podatności, którego dotyczy Zgłoszenie, nie jest spowodowane Błędem Krytycznym/Awarią lub Błędem Drobnym/Usterką, za którą odpowiedzialny jest Wykonawca, wówczas Wykonawca zobowiązany jest: a) wskazać przyczynę nieprawidłowego działania systemu poprzez wskazanie elementu, który ją powoduje, b) udzielić wsparcia Zamawiającemu lub innej osobie trzeciej wskazanej przez Zamawiającego usuwającej przyczyny Zgłoszenia, w tym udzielić takiej osobie wszelkich informacji o systemie, potrzebnych do przywrócenia jego pełnej funkcjonalności.
WAT.9	Jeżeli Wykonawca stwierdzi, iż nieprawidłowe działanie systemu SIEM, SOAR lub skanera podatności spowodowane jest okolicznościami leżącymi po stronie Oprogramowania standardowego, wówczas Wykonawca nie jest zobowiązany do naprawy Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki, jeżeli nie jest w stanie jej wykonać ze względu na prawa osób trzecich. Wykonawca jest zobowiązany do dostarczenia Obejścia w Czasie Obejścia, w szczególności do zmodyfikowania Systemu SIEM, SOAR lub skanera podatności tak, aby zapewnić jego działanie mimo istnienia Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki w Oprogramowaniu standardowym.

Identyfikator	Opis wymagania
WAT.10	Naprawa lub Obejście, które Wykonawca wdrożył, a które zostało odrzucona przez Zamawiającego ze względu na fakt, iż testy przeprowadzone przez Zamawiającego wykazują, że Błąd Krytyczny/Awaria lub Błąd Drobny/Usterka nadal występuje, trwa do czasu jego skutecznego wykonania.
WAT.11	Przez okres trwania Umowy Wykonawca zobowiązany jest przyjmować zapytania Zamawiającego dotyczące realizacji usług w ramach usług wsparcia technicznego. Zapytania składane będą: a) za pośrednictwem aplikacji serwisowej (interfejsu helpdesk), b) za pośrednictwem poczty elektronicznej na wskazany przez Wykonawcę adres email.
WAT.12	Zapytanie składane przez Zamawiającego będzie zawierać co najmniej: 1) Opis prac jakie Zamawiający chce zlecić. 2) Określenie oczekiwań Zamawiającego co do produktów i prac oraz sposobu ich wykonania i prowadzenia. 3) Termin zakończenia prac. 4) Inne kwestie istotne dla Zamawiającego
WAT.13	Wykonawca udzieli odpowiedzi na zapytanie Zamawiającego w terminie 3 Dni Roboczych od dnia jego złożenia.
WAT.14	Odpowiedź na zapytanie zawierać będzie: 1) Propozycję sposobu wykonania zlecenia. 2) Termin wykonania prac. 3) Koszt wykonania prac
WAT.15	Zamawiający w terminie 3 Dni Roboczych od dnia otrzymania odpowiedzi na zapytanie udzieli Zlecenia na wykonanie dodatkowych prac.
WAT.16	Brak ustosunkowania się przez Zamawiającego do odpowiedzi na zapytanie oznacza rezygnację z realizacji Zlecenia.
WAT.17	Realizacja Zlecenia potwierdzona będzie przez obie strony Protokołem Odbioru Miesięcznego za wsparcie.
WAT.18	Podstawą do ustalenia wysokości wynagrodzenia z tytułu Zlecenia będzie czasochłonność wykonania danego Zlecenia, zaakceptowana przez Zamawiającego.
WAT.19	Zamawiający dokona płatności jedynie za faktycznie wykorzystaną liczbę godzin prac zleconych.
WAT.20	Wykonawca musi zrealizować wszystkie złożone przez Zamawiającego Zlecenia.
WAT.21	Produkty wykonane lub dostarczone w ramach Zgłoszenia lub Zlecenia objęte zostaną Gwarancją, bez zmiany wysokości wynagrodzenia przysługującego Wykonawcy z tego tytułu.
WAT.22	Autorskie prawa majątkowe do produktów wykonanych lub dostarczonych w ramach Zlecenia będą przeniesione na Zamawiającego z chwilą podpisania Protokołu odbioru miesięcznego za wsparcie.
WAT.23	Po przeprowadzeniu implementacji poprawek w ramach Zgłoszeń i realizacji Zleceń Wykonawca musi uaktualnić Dokumentację w zakresie wykonanych zmian

VIII. Harmonogram ramowy

Etap	Zadania	Termin
1	1) Dostarczenie licencji na oprogramowanie systemu SIEM i SOAR. 2) Wdrożenie i konfiguracja systemu SIEM zgodnie z przedstawionymi wymaganiami. 3) Wdrożenie i konfiguracja skanera podatności zgodnie z przedstawionymi wymaganiami. 4) Dostarczenie dokumentacji przedwdrożeniowej oraz dokumentacji technicznej i dokumentacji użytkownika.	
2	1) Wdrożenie i konfiguracja systemu SOAR zgodnie z przedstawionymi wymaganiami 2) Dostarczenie dokumentacji powdrożeniowej zgodnie z przedstawionymi wymaganiami. 3) Przeprowadzenie szkolenia/warsztatu zgodnie z przedstawionymi wymaganiami	

IX. Szkolenia/warsztaty

Identyfikator	Opis wymagania
WSZK.01	Wykonawca zapewni bezpłatne 4-dniowe certyfikowane warsztaty (4 dni x 8h) w zakresie użytkowania i administrowania wdrożonym systemem SIEM i SOAR.
WSZK.02	Warsztaty zostaną przeprowadzone dla łącznie 5 osób i będą uwzględniać informacje z zakresu wdrożonego systemu SIEM i SOAR (m.in. zarządzanie incydentami bezpieczeństwa, korzystanie ze scenariuszy obsługi incydentów, kompletowanie informacji potrzebnych do opracowania raportu o incydencie, szacowanie ryzyka, itp.).
WSZK.03	Po zakończeniu warsztatów, uczestnicy otrzymają zaświadczenia potwierdzające uczestnictwo w szkoleniach/warsztatach oraz nabycie umiejętności obsługi systemu SIEM i SOAR.
WSZK.04	Warsztaty odbędą się w siedzibie Zamawiającego lub, ze względu na panujący stan epidemiczny oraz wprowadzone przez władze państwa ograniczenia, w formie zdalnej.
WSZK.05	Wykonawca dla każdego uczestnika dostarczy materiały szkoleniowe w języku polskim w postaci elektronicznej.
WSZK.06	Szczegółowy plan, zakres i terminy szkoleń/warsztatów zostaną uzgodnione przez Wykonawcę z Zamawiającym.

X. Dokumentacja

Identyfikator	Opis wymagania

Identyfikator	Opis wymagania
WDOK.01	Wykonawca dostarczy dokumentację obejmującą: a) projekt wdrożenia rozwiązania w infrastrukturze Zamawiającego, b) dokumentacja powdrożeniową, c) dokumentację techniczną umożliwiająca Zamawiającemu samodzielną administracje rozwiązaniem, d) dokumentację użytkownika, zawierającą typowe scenariusze użycia SIEM i SOAR, a także przekaże Zamawiającemu wszelkie, niezbędne do poprawnego korzystania z wdrożonego rozwiązania, informacje o specyfice systemu oraz informacje techniczne na temat jego prawidłowej eksploatacji.
WDOK.02	Wszelka dokumentacja wytworzona przez Wykonawcę musi być sporządzona w języku polskim.
WDOK.03	Dokumentacja musi być w formacie Microsoft Word z obsługą trybu rejestracji zmian.
WDOK.04	Wszelka dokumentacja musi charakteryzować się wysoką jakością i czytelnością.
WDOK.05	Dodatkowe formaty zapisu dokumentacji np. diagramy UML lub formaty wektorowe należy dołączyć na odrębnym nośniku danych. Pliki powinny być możliwe do otwarcia/importu przez: MS Project, MS Visio.

XI. Procedury odbioru

Procedurom odbioru przedmiotu zamówienia podlegają następujące elementy:

1. Dostawa licencji na oprogramowanie systemu SIEM wraz z modułem SOAR.
2. Wdrożenie i konfiguracja systemu SIEM.
3. Dostawa, wdrożenie i konfiguracja darmowego skanera podatności open source.
4. Wdrożenie i konfiguracja modułu SOAR.
5. Dostarczenie dokumentacji – projektu wdrożenia, dokumentacji technicznej, dokumentacji dla użytkownika, dokumentacji powdrożeniowej.
6. Szkolenie/warsztaty z obsługi SIEM i SOAR.

1. Wymagania ogólne – Procedury Odbioru

Identyfikator	Opis wymagania
WPO.1	Odbiór każdego elementu realizacji przedmiotu zamówienia dotyczący wdrożenia i konfiguracji oprogramowania musi być potwierdzony Protokołem Odbioru Jakościowego.
WPO.2	Odbiór poszczególnych elementów realizacji przedmiotu zamówienia musi następować po kolei zgodnie z harmonogramem ramowym.
WPO.3	Odbiór dokumentacji musi być potwierdzony Protokołem Odbioru Dokumentacji.
WPO.4	Odbiór licencji musi być potwierdzony Protokołem Odbioru Ilościowego.
WPO.5	Odbiór szkoleń w formie warsztatów musi być potwierdzony Protokołem Odbioru Szkolenia.

Identyfikator	Opis wymagania
WPO.6	Odbiór Zleceń wykonania prac dodatkowych w ramach Usług wsparcia technicznego musi być potwierdzony Protokołem Odbioru Miesięcznego za wsparcie.
WPO.7	Odbiór końcowy przedmiotu zamówienia musi być potwierdzony Protokołem Odbioru Końcowego.

2. Procedura odbioru Etap 1

Identyfikator	Opis wymagania
WPOE2.1	W etapie 1 zostanie zrealizowane: 1) Dostarczenie licencji na oprogramowanie systemu SIEM i SOAR. 2) Wdrożenie i konfiguracja systemu SIEM. 3) Wdrożenie i konfiguracja skanera podatności. 4) Dostarczenie dokumentacji przedwdrożeniowej oraz dokumentacji technicznej i dokumentacji użytkownika dla systemu SIEM.
WPOE2.2	Odbiór dostarczonych dokumentów potwierdzony zostanie Protokołem Odbioru Dokumentacji.
WPOE2.3	Odbiór dostarczonych licencji potwierdzony zostanie Protokołem Ilościowym.
WPOE2.4	Odbiór wdrożenia systemu SIEM zostanie potwierdzony Protokołem Odbioru Jakościowego.
WPOE2.5	Odbiór wdrożenia skanera podatności zostanie potwierdzony Protokołem Odbioru Jakościowego.

3. Procedura odbioru Etap 2

Identyfikator	Opis wymagania
WPOE2.1	W etapie 2 zostanie zrealizowane: 1) Wdrożenie i konfiguracja systemu SOAR zgodnie z przedstawionymi wymaganiami 2) Dostarczenie dokumentacji powdrożeniowej zgodnie z przedstawionymi wymaganiami 3) Przeprowadzenie szkolenia/warsztatu zgodnie z przedstawionymi wymaganiami
WPOE2.2	Odbiór dostarczonych dokumentów potwierdzony zostanie Protokołem Odbioru Dokumentacji.
WPOE2.3	Odbiór wdrożenia systemu SOAR zostanie potwierdzony Protokołem Odbioru Jakościowego.
WPOE2.4	Odbiór szkoleń w formie warsztatów zostanie potwierdzony Protokołem Odbioru Szkolenia.
WPOE2.5	Odbiór końcowy przedmiotu zamówienia musi być potwierdzony Protokołem Odbioru Końcowego.

4. Procedury Odbioru – Odbiór jakościowy

Identyfikator	Opis wymagania
WPOJ.1	Na 3 Dni Robocze przed terminem odbioru jakościowego, Wykonawca zobowiązany jest przekazać informację o planowanym odbiorze oraz osobach realizujących odbiór jakościowy.
WPOJ.2	Odbiór wdrożenia i konfiguracji systemu SIEM, SOAR oraz skanera podatności będzie polegał na sprawdzeniu przez Wykonawcę w obecności Zamawiającego poprawności działania zainstalowanego oprogramowania oraz zgodności działania i konfiguracji z wymaganiami Zamawiającego.
WPOJ.3	Odbiór wdrożenia i konfiguracji systemu SIEM, SOAR oraz skanera podatności potwierdzony zostanie Protokołem Jakościowym, w którym Zamawiający określa czy: 1) Odbiera wdrożenie systemu SIEM bez zastrzeżeń. 2) Odbiera wdrożenie systemu SIEM z zastrzeżeniami.
WPOJ.4	W przypadku uwag do odbioru jakościowego, Zamawiający dołącza do Protokołu Jakościowego ich wykaz.
WPOJ.5	Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Jakościowego z zastrzeżeniami.
WPOJ.6	Ostateczną datą odbioru jakościowego jest data podpisania Protokołu Odbioru Jakościowego bez zastrzeżeń.

5. Procedury odbioru – odbiór dokumentacji

Identyfikator	Opis wymagania
WPOD.1	Wykonawca, z 3-cio dniowym wyprzedzeniem, zobowiązany jest przekazać informację o planowanym terminie przekazania Dokumentacji do akceptacji.
WPOD.2	Dla Dokumentacji zawierającej maksymalnie 300 stron, w terminie 5 Dni Roboczych od dnia przekazania Dokumentacji, Zamawiający przekazuje Wykonawcy Protokół Odbioru Dokumentacji, w którym określa czy: 1) Odbiera Dokumentację bez zastrzeżeń. 2) Odbiera Dokumentację z zastrzeżeniami
WPOD.3	Dla Dokumentacji zawierającej więcej niż 300 stron, termin odbioru Dokumentacji zostanie ustalony wspólnie przez Zamawiającego i Wykonawcę, jednak nie może być on dłuższy niż 10 Dni Roboczych.
WPOD.4	W przypadku uwag do Dokumentacji, Zamawiający dołącza do Protokołu Odbioru Dokumentacji ich wykaz.
WPOD.5	Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag i przekazać poprawioną Dokumentację wraz z odniesieniem się do uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Dokumentacji z zastrzeżeniami.
WPOD.6	Ostateczną datą odbioru Dokumentacji jest data podpisania Protokołu Odbioru Dokumentacji bez zastrzeżeń.

6. Procedury odbioru – odbiór szkolenia / warsztatu

Identyfikator	Opis wymagania
WPOS.1	Do Protokołu Odbioru Szkolenia Wykonawca musi dołączyć listy obecności uczestników szkolenia/warsztatów oraz kopie imiennych zaświadczeń o ukończeniu szkolenia/warsztatów wszystkich uczestników.
WPOS.2	Zakończenie Szkolenia w formie warsztatów potwierdzone zostanie Protokołem Odbioru Szkolenia, w którym Zamawiający określa czy: 1) Odbiera szkolenia/warsztaty bez zastrzeżeń. 2) Odbiera szkolenia/warsztaty z zastrzeżeniami.
WPOS.3	Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Szkolenia z zastrzeżeniami.
WPOS.4	Ostateczną datą odbioru szkoleń/warsztatów jest data podpisania Protokołu Odbioru Szkolenia bez zastrzeżeń.

7. Procedury odbioru – odbiór końcowy

Identyfikator	Opis wymagania
WPOK.1	Kryterium odbioru końcowego systemu SIEM, SOR oraz skanera podatności będzie podpisanie bez zastrzeżeń: Protokołów Odbioru Jakościowego, Protokołów Odbioru Ilościowego, Protokołów Odbioru Dokumentacji, Protokołów Odbioru szkolenia z realizacji każdego Etapu przedmiotu zamówienia.
WPOK.2	Odbiór końcowy potwierdzony zostanie Protokołem Odbioru Końcowego w którym Zamawiający określa czy: 1) Dokonuje odbioru przedmiotu zamówienia bez zastrzeżeń. 2) Dokonuje odbioru przedmiotu zamówienia z zastrzeżeniami.
WPOK.3	W przypadku uwag do odbioru końcowego, Zamawiający dołącza do Protokołu Odbioru Końcowego ich wykaz.
WPOK.4	Wykonawca jest zobowiązany odnieść się do przekazanych przez Zamawiającego uwag w terminie 3 Dni Roboczych od dnia przekazania przez Zamawiającego Protokołu Odbioru Końcowego z zastrzeżeniami.
WPOK.5	Ostateczną datą odbioru końcowego jest data podpisania Protokołu Odbioru Końcowego bez zastrzeżeń.

8. Procedura Odbioru – Usługi wsparcia technicznego

Identyfikator	Opis wymagania
WPOR.1	
WPOR.2	
WPOR.3	

XII. Gwarancja

1. Gwarancja - Wymagania ogólne

Identyfikator	Opis wymagania
WGW.1	Wykonawca udzieli 24 miesięcznej Gwarancji na dostarczone systemy SIEM i SOAR oraz skaner podatności.
WGW.2	Wykonawca zapewni 24-to miesięczną Gwarancję producenta na Oprogramowanie Standardowe.
WGW.3	Wykonawca udzieli 24 miesięcznej rękojmi na: 1) Oprogramowanie standardowe. 2) Oprogramowanie dedykowane (SIEM, SOAR i skaner podatności).
WGW.4	Wykonawca będzie świadczył usługi wsparcia technicznego dla systemu SIEM i SOAR wraz ze skanerem podatności w okresie obowiązywania Umowy.
WGW.5	Gwarancja na Oprogramowanie standardowe będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM.
WGW.6	Gwarancja na dostarczone Oprogramowanie SIEM, SOAR oraz skaner podatności będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM.
WGW.7	Rękojmia będzie liczona od dnia podpisania Protokołu Odbioru Jakościowego systemu SIEM.
WGW.8	Błędy Krytyczne i Błędy Drobne Oprogramowania dedykowanego i Oprogramowania standardowego będą usuwane zgodnie z warunkami producenta, przy czym warunki te nie mogą być gorsze niż wymagania dotyczące Gwarancji.
WGW.9	Zakres świadczeń w ramach Gwarancji obejmuje: 1) Usuwanie Błędów Krytycznych i Błędów Drobnych Oprogramowania standardowego oraz Oprogramowania SIEM, SOAR oraz skanera podatności zgodnie z Czasami Reakcji, Czasami Naprawy, Czasami Obejścia i Maksymalnymi czasami Obejścia dla poszczególnych kategorii błędów. 2) Dostarczanie, instalację i konfigurację nowych wersji Oprogramowania standardowego oraz Oprogramowania SIEM, SOAR oraz skanera podatności. 3) Prowadzenie wszelkich działań prewencyjnych mających na celu wydłużenie czasu bezawaryjnej pracy przedmiotu zamówienia. 4) Odzyskiwanie danych systemu SIEM i SOAR utraconych lub uszkodzonych w wyniku Błędów Krytycznych/Awarii i Błędów Drobnych/Usterek Oprogramowania Standardowego lub Oprogramowania SIEM, SOAR oraz skanera podatności.
WGW.10	Wykonawca zobowiązuje się do świadczenia usług w ramach Gwarancji w sposób zapobiegający utracie jakichkolwiek danych przetwarzanych w systemie SIEM.
WGW.11	Wykonawca w ramach Gwarancji pokryje wszystkie koszty związane z naprawą, m.in. koszty transportu, ubezpieczenia, robocizny.

2. Gwarancja – Oprogramowanie standardowe

Identyfikator	Opis wymagania
WGWOS.1	Wykonawca zapewni elektroniczny dostęp do informacji na temat posiadanego Oprogramowania standardowego oraz biuletynów technicznych, poprawek, aktualizacji, nowych wersji Oprogramowania standardowego.
WGWOS.2	Wykonawca w przypadku Oprogramowania standardowego: 1) Opracowuje i uzgadnia z Zamawiającym plan obsługi serwisowej (raz w roku). 2) Dostarcza aktualizacje, nowe wersje oraz zmiany w Oprogramowaniu standardowym, opracowane przez producenta podczas trwania Gwarancji. 3) Zapewnia, że dostarczane aktualizacje, nowe wersje lub zmiany są produktami wykonanymi przez producenta, a tym samym nie naruszają praw własności intelektualnej oraz że Wykonawca posiada prawo do ich dostarczania osobom trzecim. 4) W ciągu każdego roku trwania Umowy opracowuje plan aktualizacji Oprogramowania standardowego. 5) Informuje o najlepszych praktykach i zasadach postępowania.
WGWOS.3	Wykonawca musi zapewnić wsparcie producenta w przypadku gdy zgodnie z licencją producenta dostęp do aktualizacji Oprogramowania standardowego takiego wsparcia wymaga.
WGWOS.4	Wykonawca musi zapewnić subskrypcje Oprogramowania standardowego w przypadku gdy są one niezbędne do poprawnego działania wymaganych funkcjonalności systemu.

3. Gwarancja – Oprogramowanie SIEM, SOAR i skaner podatności

Identyfikator	Opis wymagania
WGWSI.1	Wykonawca ponosi odpowiedzialność za poprawne funkcjonowanie Oprogramowania SIEM, SOAR oraz skaner podatności będącego przedmiotem zamówienia.
WGWSI.2	Po usunięciu każdego Błędu Krytycznego/Awarii lub Błędu Drobnego/Usterki Wykonawca zobowiązany jest do przywrócenia prawidłowego funkcjonowania Oprogramowania SIEM, SOAR oraz skanera podatności.

XIII. SLA

Identyfikator	Opis wymagania
WSLA.01	SLA dla oprogramowania będzie liczone w okresie jednego roku.
WSLA.02	W uzasadnionych przypadkach Zamawiający wraz z Wykonawcą mogą podjąć decyzję o wydłużeniu Czasu Naprawy, Czasu Obejścia, Maksymalnego czasu Obejścia.

Identyfikator	Opis wymagania
WSLA.03	Okna serwisowe związane z konserwacją/naprawą/rekonfiguracją Sytemu nie podlegają uwzględnianiu w obliczeniu SLA. Termin i zakres prac realizowanych w ramach okna serwisowego wymaga uzyskania przez Wykonawcę uprzedniej akceptacji Zamawiającego.

Kategoria	Czas Reakcji	Czas Naprawy	Czas Obejścia	Maksymalny czas Obejścia
Błąd Krytyczny/Awaria	2 godziny w Dniu Roboczym	24 godziny	12 godzin	7 Dni Roboczych
Błąd Drobny/Usterka	2 godziny w Dniu Roboczym	48 godzin	12 godzin	14 Dni Roboczych

XIV. Bezpieczeństwo przetwarzanych danych

Identyfikator	Opis wymagania
WBPD.01	Wykonawca zobowiązany jest do przestrzegania, przekazanych w trakcie realizacji przedmiotu zamówienia, zasad i przepisów dotyczących bezpieczeństwa informacji oraz systemów informatycznych, obowiązujących u Zamawiającego, oraz innych zasad związanych z wykonywaniem czynności na terenie obiektów Zamawiającego. Zobowiązanie to dotyczy wszystkich osób, z pomocą których Wykonawca będzie realizował przedmiot zamówienia.
WBPD.02	System SIEM musi być w pełni zgodny z zasadami bezpieczeństwa zdefiniowanymi w przekazanych przez Zamawiającego instrukcjach i procedurach. Z uwagi na zakres Polityki Bezpieczeństwa Danych Osobowych (PBDO) Zamawiającego, zasady i reguły określone w PBDO podlegają ochronie przed ujawnieniem lub udostępnieniem nieupoważnionej lub nieuprawnionej osobie lub nieuprawnionemu podmiotowi zewnętrznemu, dlatego dokumenty te zostaną przekazane Wykonawcy po podpisaniu Umowy na realizację przedmiotu zamówienia.
WBPD.03	Przesyłanie danych w obrębie systemu SIEM i SOAR musi odbywać się w dedykowanej sieci Zamawiającego - bezpiecznymi kanałami, szyfrowanymi i chronionymi przed nieuprawnionym dostępem oraz zapewniającymi poufność, integralność i dostępność danych osobowych.
WBPD.04	Wszystkie dane, które będą udostępnione w systemie SIEM i SOAR muszą być chronione przed nieuprawnionym odczytem poprzez mechanizmy logowania z wykorzystaniem unikalnego identyfikatora oraz hasła. Wytyczne dotyczące sposobu budowania identyfikatorów i haseł zostaną przekazane przez Zamawiającego.

Identyfikator	Opis wymagania
WBPD.05	System SIEM i SOAR musi zapewniać logowanie wszystkich udanych i nieudanych prób dostępu do systemu z uwzględnieniem informacji o użytkowniku końcowym, dacie i czasie logowania oraz adresu IP z którego nastąpiła próba logowania.
WBPD.06	System SIEM i SOAR musi umożliwiać pełną identyfikację użytkownika końcowego i czasu wykonania każdej zmiany w bazie danych systemu, w szczególności operacji wstawiania rekordów, aktualizacji rekordów, tak aby zagwarantować pełną rozliczalność systemu.

XV. Zobowiązania Wykonawcy

W ramach realizacji Przedmiotu zamówienia Wykonawca zobowiązany jest do przestrzegania i realizacji poniższych zasad:

Identyfikator	Opis wymagania
WZW.01	Przedmiot zamówienia musi zostać zrealizowany przez Wykonawcę z najwyższą starannością, efektywnością oraz zgodnie z najlepszą praktyką i wiedzą zawodową.
WZW.02	Całość Przedmiotu zamówienia musi zostać zrealizowana zgodnie z terminami określonymi w OPZ.
WZW.03	Wykonawca jest zobowiązany do dokonywania wszelkich niezbędnych ustaleń mogących wpływać na Przedmiot Zamówienia z Zamawiającym.
WZW.04	Wykonawca sprawnie i terminowo zrealizuje Przedmiot zamówienia, w tym uwzględni w trakcie jego realizacji wszystkie uwagi zgłaszane przez Zamawiającego.
WZW.05	Wykonawca, na każdym etapie umowy, udzieli Zamawiającemu wszelkich informacji na temat stanu realizacji Przedmiotu zamówienia.

XVI. Zobowiązania Zamawiającego

W ramach realizacji Przedmiotu zamówienia Zamawiający zobowiązany jest do:

Identyfikator	Opis wymagania
WZZ.01	Udostępnienia wszelkich materiałów, danych, dokumentacji i informacji będących w posiadaniu Zamawiającego, które są niezbędne celem realizacji Przedmiotu zamówienia.
WZZ.02	Informowania Wykonawcy o wszelkich czynnościach, które mogą mieć wpływ na realizację Przedmiotu zamówienia przez Wykonawcę.
WZZ.03	Udostępnienia obiektów, sprzętu, oprogramowania i dokumentacji, które są niezbędne do realizacji Przedmiotu zamówienia zgodnie z polityką bezpieczeństwa i regulacjami wewnętrznymi, obowiązującymi u Zamawiającego.