OPIS PRZEDMIOTU ZAMÓWIENIA

Dostawa licencji systemu orkiestracji, automatyzacji i reagowania na incydenty bezpieczeństwa (SOAR) wraz ze wsparciem producenta, szkoleniem oraz usługą wdrożenia w dwóch niezależnych sieciach IT i OT

1. Przedmiot zamówienia

1.1. Przedmiotem zamówienia jest dostawa licencji wieczystych na oprogramowanie klasy SOAR (Security Orchestration, Automation and Response) dla dwóch niezależnych instancji – w sieci IT oraz w sieci OT Zamawiającego – wspomagające pracę zespołu reagowania na incydenty bezpieczeństwa Zamawiającego, wraz ze wsparciem producenta, szkoleniem oraz usługą wdrożenia.

1.2. W skład przedmiotu zamówienia wchodzą:

Lp.	Element przedmiotu zamówienia	Ilość
1.	Licencja wieczysta na oprogramowanie SOAR – zgodnie z rozdz. 2 i 3	2 kpl. (1 – sieć IT, 1 – sieć OT)
2.	Wsparcie producenta oprogramowania SOAR dla obu instancji (IT i OT) – zgodnie z rozdz. 4	24 miesiące
3.	Voucher szkoleniowy – zgodnie z rozdz. 5	2 uczestników
4.	Usługa wdrożenia systemu SOAR w dwóch niezależnych sieciach IT i OT	1 usługa

1.4. Zamówienie obejmuje dostawę licencji dla dwóch instancji systemu SOAR: jednej przeznaczonej dla sieci IT i jednej dla sieci OT Zamawiającego. Instancje muszą działać jako dwa całkowicie niezależne systemy, zgodnie z pkt 2.7 i rozdz. 6. Wymagania z rozdz. 3 dotyczą każdej z instancji.

1.5. Kod CPV: 48730000-4 Pakiety oprogramowania zabezpieczającego; 72268000-1 Usługi dostawy oprogramowania; 80533100-0 Usługi szkolenia w zakresie komputerów; 72265000-0 Usługi konfiguracji oprogramowania.

2. Wymagania ogólne

2.1. Licencje muszą być licencjami wieczystymi (udzielonymi na czas nieoznaczony), wystawionymi na Zamawiającego, obejmującymi co najmniej **2** użytkowników (analityków / operatorów) instancji IT oraz co najmniej **2** użytkowników instancji OT. Licencje nie mogą ograniczać liczby obsługiwanych incydentów, scenariuszy ani integracji.

2.2. Po zakończeniu okresu wsparcia producenta każda z instancji musi nadal działać w pełnym zakresie funkcjonalnym, z wykorzystaniem ostatniej zainstalowanej wersji oprogramowania, bez konieczności ponoszenia dodatkowych opłat.

2.3. Oprogramowanie musi być instalowane w infrastrukturze Zamawiającego (on-premise), w środowisku wirtualizacyjnym Zamawiającego, odrębnym dla sieci IT i dla sieci OT. Działanie funkcji systemu nie może wymagać stałego połączenia z chmurą producenta; dotyczy to także licencjonowania i aktywacji licencji. Instancja OT musi zapewniać pełną funkcjonalność w środowisku bez dostępu do Internetu, z możliwością aktualizacji oprogramowania i zawartości (integracji, scenariuszy, skryptów) w trybie offline.

2.4. Wykonawca wskaże w ofercie minimalne wymagania sprzętowe i systemowe (procesor, pamięć RAM, przestrzeń dyskowa, system operacyjny) niezbędne do działania każdej z instancji w zakresie wymaganym w OPZ dla wskazanej w pkt 2.1 liczby użytkowników.

2.5. Oprogramowanie musi być dostarczone w najnowszej wersji dostępnej na dzień dostawy. Interfejs użytkownika musi być dostępny w języku polskim lub angielskim, a dokumentacja – w języku polskim lub angielskim (dopuszcza się wersję elektroniczną).

2.6. Licencja i wsparcie muszą pochodzić z oficjalnego kanału dystrybucji producenta na terenie Unii Europejskiej. Wykonawca przekaże dokumenty potwierdzające udzielenie licencji i rejestrację wsparcia u producenta na rzecz Zamawiającego.

2.7. Instancje dla sieci IT i OT muszą być od siebie całkowicie niezależne. Każda instancja musi działać samodzielnie, z własną bazą danych, kontami użytkowników, konfiguracją i licencją, bez wspólnej konsoli zarządzania, synchronizacji danych lub konfiguracji ani połączeń sieciowych między instancjami. Zamawiający nie dopuszcza realizacji separacji sieci IT i OT wyłącznie w trybie multi-tenant w ramach jednej instancji.

3. Wymagania funkcjonalne systemu SOAR

Oferowane oprogramowanie musi spełniać co najmniej poniższe wymagania minimalne, odrębnie w każdej z instancji (IT i OT).

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
A. Obsługa incydentów		
1.	Oprogramowanie musi wspomagać pracę zespołu reagowania na incydenty komputerowe (SOC, CERT, CSIRT, IRT itp.), tj. procesy monitorowania bezpieczeństwa teleinformatycznego, reagowania na incydenty oraz zarządzania podatnościami, przy czym głównym celem jest standaryzacja i automatyzacja działań analityków cyberbezpieczeństwa.	
2.	Oprogramowanie musi umożliwiać automatyczne tworzenie incydentów wymagających obsłużenia na podstawie powiadomień z systemu klasy SIEM, zgłoszeń przekazywanych przez użytkowników na dedykowany adres e-mail oraz zgłoszeń przypisanych do odpowiedniej grupy w systemie typu helpdesk – co najmniej w systemie RTIR (Request Tracker for Incident Response) lub Jira. Ponadto rozwiązanie musi umożliwiać automatyczne zamykanie obsłużonego zgłoszenia w systemie typu helpdesk, co najmniej w systemie RTIR lub Jira.	
3.	Oprogramowanie musi umożliwiać ręczne utworzenie incydentu.	
4.	Oprogramowanie musi umożliwiać automatyczną oraz ręczną klasyfikację incydentów ze względu na ich krytyczność.	
5.	Oprogramowanie musi umożliwiać tworzenie własnych definicji klasyfikacji incydentów i ich krytyczności.	
6.	Oprogramowanie musi umożliwiać śledzenie czasu oraz podjętych działań w ramach utworzonego incydentu, a także raportowanie czasów Time-to-Detect oraz Time-to-Mitigate.	
7.	Oprogramowanie musi umożliwiać łączenie utworzonych incydentów, w tym inteligentne łączenie automatyczne.	
8.	Oprogramowanie musi umożliwiać automatyczne przydzielanie predefiniowanych zadań dla danych typów incydentów.	
9.	Oprogramowanie musi umożliwiać automatyczne oraz ręczne przydzielanie incydentów wymagających obsłużenia do pracowników obsługujących system.	
10.	Oprogramowanie musi umożliwiać automatyczną oraz ręczną weryfikację atrybutów charakterystycznych dla danego incydentu w wewnętrznych oraz zewnętrznych źródłach informacji.	
11.	Oprogramowanie musi posiadać wbudowaną bibliotekę minimum 5 typów incydentów, a także dostarczać specjalizowane typy incydentów związane z integrowanymi systemami, pozwalając na ich edycję lub kopiowanie w celu stworzenia własnej karty incydentu.	
12.	Oprogramowanie musi pozwalać na sprawdzenie, które incydenty nie zostały obsłużone.	
13.	Oprogramowanie musi pozwalać na automatyczne wypełnianie pól incydentu na podstawie typu incydentu lub jego atrybutów.	
14.	Oprogramowanie musi pozwalać na delegowanie zadań innym członkom zespołu SOC w ramach oceny danego incydentu.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
15.	Oprogramowanie musi pozwalać na współpracę pomiędzy członkami zespołu SOC (np. rozmowę członków zespołu na temat incydentu).	
16.	Oprogramowanie musi pozwalać na zapisywanie historycznych incydentów wraz z pełną informacją na temat podjętych działań obsługi i rozwiązania, w celu szkolenia i transferu wiedzy pomiędzy członkami zespołu SOC. Na historię incydentu składają się m.in.: wyniki działania automatycznych i ręcznych zadań określonych w scenariuszu (playbooku), komentarze analityków pracujących nad incydentem, wskaźniki zagrożenia IOC (IP, URL, domeny itd.) wyodrębniane automatycznie i wskazywane ręcznie w czasie obsługi incydentu, elementy analizy oznaczone przez analityków jako dowód w sprawie (np. zrzuty ekranu z widokiem podejrzanych stron WWW) oraz pliki dodawane do historii obsługi incydentu przez analityków.	
17.	Oprogramowanie musi pozwalać na proste wyszukiwanie incydentów na podstawie ich cech (np. przy użyciu dedykowanego języka zapytań) oraz podobieństwa do innych incydentów (related incidents).	
18.	Oprogramowanie musi pozwalać na wizualizację zależności pomiędzy podobnymi incydentami na poziomie wystąpień identycznych wskaźników.	
19.	System musi posiadać natywną integrację z MITRE ATT&CK i przypisywać do incydentów odpowiednie techniki i taktyki.	
B. Scenariusze obsługi incydentów (playbooki) i automatyzacja		
20.	Oprogramowanie musi umożliwiać tworzenie i edytowanie procedur reagowania na incydenty w postaci graficznej. System musi umożliwiać stosowanie podstawowych operatorów logicznych i matematycznych przy definicji procedur.	
21.	Oprogramowanie musi umożliwiać zaprojektowanie oraz wdrożenie automatycznych działań reagowania na dane typy incydentów.	
22.	Oprogramowanie musi umożliwiać edycję kodu źródłowego automatycznych działań reagowania. Wymaga się stosowania powszechnie używanego języka skryptowego w wersji wspieranej przez jego twórców (np. Python 3).	
23.	Oprogramowanie musi umożliwiać dwustronną komunikację z użytkownikami systemu (np. w celu zebrania dodatkowych informacji od osób związanych z incydentem) oraz z operatorami systemu SOAR, na przykład poprzez zastosowanie interaktywnych formularzy.	
24.	Oprogramowanie musi automatyzować proces analizy otrzymanych danych, realizować funkcje informacyjne oraz podejmować działania naprawcze (np. automatyczna analiza pliku w środowisku sandbox w chmurze wybranego producenta, wysłanie wiadomości e-mail do użytkownika zainfekowanej stacji końcowej z ostrzeżeniem przed otwieraniem załącznika, blokada na urządzeniu sieciowym dostępu do wskazanych usług dla wybranego użytkownika).	
25.	Oprogramowanie musi umożliwiać wykorzystanie w skryptach własnych bibliotek zewnętrznych oraz programów (np. poprzez uruchamianie skryptów we własnym kontenerze, zawierającym wymagane oprogramowanie).	
26.	Oprogramowanie musi pozwalać na kopiowanie oraz edycję istniejących scenariuszy, jak również na dodawanie nowych.	
27.	Oprogramowanie musi pozwalać na edycję i dodawanie nowych scenariuszy obsługi incydentu (tzw. playbooków) za pomocą graficznego interfejsu użytkownika, bez konieczności wykorzystania języków skryptowych lub znajomości języków programowania.	
28.	Oprogramowanie musi pozwalać na tworzenie scenariuszy zagnieżdżonych, tzn. scenariusz nadrzędny może zawierać scenariusze podrzędne uruchamiane jako pod-scenariusze. Edycja pod-scenariusza musi automatycznie obejmować wszystkie scenariusze, które go wykorzystują.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
29.	Oprogramowanie musi pozwalać na tworzenie scenariuszy zawierających: – zadania ręczne, – zadania zautomatyzowane, – zadania warunkowe automatyczne, – zadania warunkowe ręczne, – akwizycję danych przy użyciu formularzy, – filtry danych, – pod-scenariusze.	
30.	Oprogramowanie musi pozwalać na automatyczne i ręczne wykonywanie dostępnych scenariuszy.	
31.	Oprogramowanie musi pozwalać na automatyczne dokumentowanie uruchomionych scenariuszy wraz z wynikami ich działania.	
32.	Oprogramowanie musi umożliwiać wizualizację przebiegu wykonania scenariusza (wizualizację rezultatu wszystkich wykonanych oraz pominiętych zadań, operacji warunkowych, decyzji itp.).	
33.	Oprogramowanie musi pozwalać na sterowanie wykonaniem scenariusza przez operatora (zadania warunkowe ręczne) drogą korespondencyjną, m.in. z poziomu wiadomości e-mail oraz wiadomości w komunikatorze (np. Microsoft Teams, Slack, Mattermost).	
34.	Oprogramowanie musi pozwalać na uruchomienie scenariusza w trybie krokowym w celu analizy jego poprawności i usunięcia ewentualnych błędów.	
35.	Oprogramowanie musi pozwalać na ponowne uruchomienie scenariusza dla konkretnego incydentu.	
36.	Oprogramowanie musi pozwalać na zatrzymanie scenariusza w trakcie jego wykonywania.	
37.	Oprogramowanie musi pozwalać na doraźne wykonanie dowolnego zadania automatyzacyjnego przez operatora SOC, bez konieczności tworzenia nowych lub modyfikacji istniejących scenariuszy (np. przy użyciu wiersza poleceń).	
38.	Oprogramowanie musi pozwalać na proste monitorowanie stanu wykonania scenariuszy powiązanych z incydentami. W przypadku wystąpienia jakichkolwiek anomalii w trakcie wykonania scenariusza osoby odpowiedzialne za incydent muszą zostać natychmiast o tym poinformowane.	
39.	Oprogramowanie musi pozwalać na przydzielanie zadań pojedynczego scenariusza różnym członkom zespołu SOC.	
40.	Oprogramowanie musi pozwalać na przekazywanie parametrów pomiędzy zadaniami pojedynczego scenariusza.	
41.	Oprogramowanie musi pozwalać na odczytywanie wyników analizy i wykorzystanie ich w kolejnych zadaniach uruchomionego scenariusza.	
42.	Oprogramowanie musi pozwalać na sprawdzenie danych historycznych na temat uruchomionych scenariuszy i zadań.	
43.	Oprogramowanie musi pozwalać na okresowe uruchamianie scenariuszy w zdefiniowanym czasie i według harmonogramu.	
44.	Oprogramowanie musi pozwalać na rozszerzenie możliwości systemu w zakresie tworzenia i edycji scenariuszy poprzez dodanie własnych skryptów realizujących niestandardową logikę operacji warunkowych, filtrowania i modyfikacji danych, a także skryptów realizujących niestandardową prezentację danych w dashboardach, zadania wykonywane po zakończeniu obsługi incydentu itp.	
C. Integracje		
45.	Oprogramowanie musi natywnie integrować się z systemem klasy SIEM wykorzystywanym przez Zamawiającego, tj. producent oprogramowania SOAR musi oficjalnie wspierać integrację z tym systemem.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
46.	Oprogramowanie musi integrować się co najmniej z następującymi systemami Zamawiającego: – Office 365 / Microsoft Exchange (pobieranie i wysyłanie wiadomości e-mail), – Slack (wysyłanie komunikatów), – Energy Logserver.	
47.	Oprogramowanie musi umożliwiać łatwą integrację z pozostałymi systemami klasy threat intelligence / threat hunting / threat sharing za pomocą API.	
48.	Oprogramowanie musi zapewniać zestaw co najmniej 250 gotowych integracji, pozwalających na szybką, dwustronną komunikację z zewnętrznymi systemami.	
49.	Oprogramowanie musi zapewniać możliwość wglądu w kod integracji oraz jego klonowania w celu wprowadzenia modyfikacji lub napisania własnej wersji integracji.	
50.	Oprogramowanie musi pozwalać na eksport wskaźników kompromitacji (IOC) do serwerów MISP.	
51.	Oprogramowanie musi pozwalać na import zdarzeń z serwerów MISP.	
52.	Oprogramowanie musi pozwalać na eksport incydentów w formatach STIX 1 i STIX 2, CSV oraz PDF.	
53.	Oprogramowanie musi pozwalać na tworzenie wielu instancji integracji tego samego typu z rozwiązaniami firm trzecich (np. dwie integracje z serwerami IMAP lub pobieranie danych threat intelligence z dwóch źródeł w formacie JSON).	
54.	Oprogramowanie musi pozwalać na proste wprowadzanie globalnych zestawów poświadczeń w celu ułatwienia użycia wspólnego konta technicznego w wielu integracjach z systemami trzecimi.	
D. Wskaźniki (indicators) i threat intelligence		
55.	Oprogramowanie musi posiadać repozytorium wskaźników (ang. indicators), które gromadzi i koreluje wskaźniki w ramach wszystkich incydentów, alertów i źródeł danych (feedów) dostarczanych do rozwiązania.	
56.	Oprogramowanie musi umożliwiać wykonywanie scenariuszy na podstawie zestawu wskaźników określonych przez użytkownika.	
57.	Oprogramowanie musi obsługiwać formaty strukturalne, takie jak JSON, CSV, STIX 1.x i STIX 2.x, w ramach integracji ze źródłami wskaźników.	
58.	Oprogramowanie musi obsługiwać co najmniej następujące typy wskaźników: – numery kart płatniczych, – IBAN, – adres e-mail, – konto użytkownika, – identyfikatory CVE, – domena, – FQDN, – nazwa hosta, – adres IP (IPv4 oraz IPv6), – klucz i ścieżka rejestru, – URL, – CIDR.	
59.	Oprogramowanie musi umożliwiać własną definicję wskaźników, ich pól oraz skryptów reputacyjnych.	
60.	Oprogramowanie musi zapewniać użytkownikom możliwość automatycznej weryfikacji wskaźników (tzw. enrichment) poprzez wykonanie odpowiedniego scenariusza lub uruchomienie sprawdzenia na podstawie typu wskaźnika.	
E. Raporty i dashboardy		
61.	Oprogramowanie musi umożliwiać tworzenie zbiorczych raportów z utworzonych oraz obsłużonych incydentów.	

Lp.	Minimalne wymagania Zamawiającego dotyczące przedmiotu zamówienia	
62.	System musi posiadać możliwość generowania dashboardów bezpieczeństwa z danych znajdujących się w systemie SOAR, w tym statystyk, oraz możliwość tworzenia i konfiguracji widoków głównych na ekran dyspozycyjny w pomieszczeniu SOC.	
63.	Oprogramowanie musi pozwalać na tworzenie własnych: – typów incydentów, – pól i etykiet incydentów, – typów wskaźników, – pól i etykiet wskaźników, – raportów, – dashboardów.	
64.	Oprogramowanie musi posiadać zestaw przygotowanych raportów, co najmniej: – raport na temat incydentów: dzienny, 7-dniowy i 30-dniowy, – raport na temat średniego czasu rozwiązania incydentu.	
65.	Oprogramowanie musi pozwalać na tworzenie własnych raportów oraz dashboardów za pomocą predefiniowanych komponentów umożliwiających wizualizację danych (np. wykres kołowy, słupkowy, liniowy, tabela).	
66.	Oprogramowanie musi pozwalać na eksport raportów co najmniej w formacie PDF.	
F. Architektura i licencjonowanie		
67.	Oprogramowanie musi mieć możliwość działania jako platforma SOAR dla wielu instytucji lub klientów, z całkowitą separacją zasobów i przetwarzanych danych (tzw. tryb multi-tenant).	
68.	System musi umożliwiać zakup licencji wieczystej wraz ze wsparciem producenta na okres 24 miesięcy.	

W celu potwierdzenia zgodności oferowanego rozwiązania z wymaganiami Zamawiający żąda złożenia wraz z ofertą:

- wypełnionej tabeli załączonej do Formularza ofertowego (zał. 2.1), ze wskazaniem producenta, nazwy i wersji oferowanego oprogramowania;
- dokumentacji producenta (np. karty produktu, dokumentacji technicznej, opisu licencjonowania) potwierdzającej spełnienie wymagań z rozdz. 3, w tym dostępność licencji wieczystej oraz możliwość pracy i aktualizacji bez dostępu do Internetu (instancja OT);
- wykazu gotowych integracji udostępnianych przez producenta (pkt 48 tabeli) lub wskazania publicznie dostępnego katalogu integracji;
- oświadczenia producenta lub dokumentacji producenta potwierdzającej oficjalne wsparcie integracji z systemem SIEM Zamawiającego (pkt 45 tabeli) oraz z systemami wskazanymi w pkt 46 tabeli.

Jeżeli z dokumentów producenta nie wynika jednoznacznie spełnienie danego wymagania, Wykonawca może złożyć oświadczenie producenta lub jego autoryzowanego przedstawiciela.

4. Wsparcie producenta

4.1. Wykonawca zapewni wsparcie producenta oprogramowania SOAR dla obu instancji (IT i OT) przez okres 24 miesięcy, liczony od dnia podpisania protokołu odbioru licencji.

4.2. W ramach wsparcia Zamawiający otrzyma co najmniej: dostęp do nowych wersji i aktualizacji oprogramowania, w tym poprawek bezpieczeństwa, aktualizacji integracji i zawartości (typów incydentów, scenariuszy, skryptów), dostęp do bazy wiedzy i dokumentacji producenta oraz możliwość zgłaszania problemów. Dla instancji OT producent musi udostępniać aktualizacje w postaci pakietów do instalacji w trybie offline.

4.3. Zgłoszenia przyjmowane są w dni robocze, przez portal producenta, e-mailem lub telefonicznie. Czas reakcji na zgłoszenie: nie dłuższy niż **8** godzin roboczych.

5. Szkolenie

5.1. Wykonawca dostarczy voucher szkoleniowy dla 2 uczestników w zakresie użytkowania i administrowania systemem SOAR, obejmujący zagadnienia niezbędne do obsługi obu instancji. Voucher musi być ważny nie krócej niż 12 miesięcy od dnia jego przekazania.

5.2. Szkolenie odbędzie się w formie zdalnej, w terminie uzgodnionym z Zamawiającym.

5.3. Szkolenie musi być prowadzone w języku polskim.

5.4. Każdy uczestnik szkolenia otrzyma materiały szkoleniowe przygotowane w języku polskim lub angielskim.

5.5. Osoby prowadzące szkolenie muszą posiadać certyfikat wystawiony przez producenta oferowanego rozwiązania, potwierdzający ich kompetencje w zakresie użytkowania i administrowania systemem. Wykonawca przekaże kopie certyfikatów przed rozpoczęciem szkolenia.

6. Wdrożenie w sieciach IT i OT

6.2. Zasady wdrożenia w sieciach IT i OT

6.2.1. Wdrożenie obejmuje dwa niezależne środowiska: sieć IT oraz sieć OT Zamawiającego. W każdej z sieci Wykonawca wdroży odrębną instancję systemu SOAR, zgodnie z pkt 2.7.

6.2.2. W trakcie prac Wykonawca nie może zestawiać połączeń między siecią IT a siecią OT, także tymczasowych, ani podłączać do sieci OT urządzeń lub nośników, które wcześniej były wykorzystywane w sieci IT, bez zgody Zamawiającego. Pakiety instalacyjne i aktualizacyjne dla instancji OT będą przenoszone w sposób uzgodniony z Zamawiającym, po weryfikacji ich integralności (suma kontrolna lub podpis producenta).

6.2.3. Instancja IT zostanie zintegrowana z systemami działającymi w sieci IT, a instancja OT – wyłącznie z systemami działającymi w sieci OT, w szczególności z systemem SIEM obsługującym sieć OT oraz systemami monitorowania bezpieczeństwa sieci OT. Integracje instancji OT wymagające dostępu do Internetu lub usług chmurowych (np. analiza w środowisku sandbox w chmurze, zewnętrzne źródła informacji o zagrożeniach) zostaną wyłączone albo zastąpione źródłami lokalnymi, aktualizowanymi w trybie offline.

6.2.4. W instancji OT scenariusze nie mogą automatycznie wykonywać działań naprawczych wpływających na pracę sieci OT lub urządzeń sterowania procesem (m.in. sterowników PLC, RTU, serwerów SCADA, stacji HMI). Każde takie działanie (np. blokada ruchu, izolacja hosta, wyłączenie konta) musi być poprzedzone zadaniem warunkowym ręcznym, wymagającym zatwierdzenia przez upoważnionego operatora. Automatyczne działania naprawcze można włączyć wyłącznie dla systemów wskazanych przez Zamawiającego na piśmie.

6.2.5. Prace w sieci OT Wykonawca będzie prowadził wyłącznie w oknach serwisowych uzgodnionych z Zamawiającym, zgodnie z obowiązującymi u Zamawiającego procedurami bezpieczeństwa, w sposób niepowodujący przerw ani zakłóceń w procesie technologicznym.

6.3. Zakres wdrożenia (odrębnie dla sieci IT i dla sieci OT)

6.3.1. Opracowanie harmonogramu wdrożenia systemu SOAR w obu sieciach.

6.3.2. Przeprowadzenie analizy przedwdrożeniowej oraz opracowanie odrębnego projektu technicznego wdrożenia dla sieci IT i dla sieci OT, przedkładanego do akceptacji Zamawiającego. Prace instalacyjne mogą rozpocząć się po akceptacji projektu.

6.3.3. Instalacja i konfiguracja każdej z instancji w środowisku Zamawiającego, w tym konfiguracja kont i ról użytkowników oraz utwardzenie konfiguracji (zmiana domyślnych haseł, szyfrowany dostęp do interfejsów, wyłączenie zbędnych usług). Dla instancji OT – konfiguracja pracy bez dostępu do Internetu.

6.3.4. Podłączenie do każdej z instancji systemów wskazanych w OPZ działających w danej sieci, w szczególności systemu klasy SIEM, systemów wskazanych w pkt 46 tabeli w rozdz. 3, systemu typu helpdesk oraz dedykowanej skrzynki e-mail do przyjmowania zgłoszeń – w zakresie, w jakim systemy te są dostępne w danej sieci.

6.3.5. Ustalenie wspólnie z Zamawiającym oraz zaimplementowanie w każdej z instancji właściwej klasyfikacji incydentów i ich krytyczności, z uwzględnieniem w instancji OT typów incydentów charakterystycznych dla sieci przemysłowych.

6.3.6. Skonfigurowanie dla podłączonych systemów typów incydentów, scenariuszy obsługi (playbooków), raportów oraz dashboardów, z wykorzystaniem gotowych komponentów dostarczonych wraz z systemem.

6.3.7. Jeżeli oferowany system nie posiada gotowych integracji, scenariuszy, raportów lub dashboardów dla wskazanych systemów, Wykonawca jest zobowiązany do ich implementacji na etapie wdrożenia.

6.3.8. Na etapie analizy przedwdrożeniowej Wykonawca przedstawi do akceptacji Zamawiającego listę proponowanych scenariuszy obsługi incydentów, raportów oraz dashboardów odnoszących się do podłączonych systemów, obejmującą co najmniej **2** scenariuszy dla sieci IT i co najmniej **2** scenariuszy dla sieci OT.

6.3.9. Przygotowanie i przeprowadzenie scenariuszy testowych weryfikujących wydajność i poprawność wdrożonego systemu w każdej z sieci. Proponowane scenariusze testowe zostaną przedłożone Zamawiającemu do akceptacji i muszą obejmować co najmniej:

- utworzenie incydentu z systemu SIEM, ze zgłoszenia e-mail i z systemu helpdesk oraz automatyczne zamknięcie zgłoszenia w systemie helpdesk;
- wykonanie scenariusza z zadaniami automatycznymi i ręcznymi oraz wzbogacenie wskaźników;
- w sieci OT – zatrzymanie scenariusza przed działaniem naprawczym do czasu zatwierdzenia przez operatora, zgodnie z pkt 6.2.4;
- aktualizację instancji OT w trybie offline;
- brak dostępu do interfejsów zarządzania spoza wyznaczonego segmentu zarządzania oraz brak połączeń między instancjami IT i OT.

6.3.10. Przekazanie odrębnej dla sieci IT i dla sieci OT dokumentacji powykonawczej w języku polskim, obejmującej co najmniej opis architektury i konfiguracji, wykaz integracji, kont technicznych i ról, opis wdrożonych scenariuszy, protokoły z testów oraz procedury administracyjne (aktualizacja – dla sieci OT również w trybie offline, kopia zapasowa i odtworzenie konfiguracji). Hasła zostaną przekazane w sposób uzgodniony z Zamawiającym, odrębnie od dokumentacji.

6.3.11. Osoby realizujące wdrożenie po stronie Wykonawcy przed przystąpieniem do prac podpiszą zobowiązanie do zachowania poufności informacji uzyskanych w trakcie realizacji zamówienia, w szczególności dotyczących architektury i zabezpieczeń sieci IT i OT.

6.3.12. Wykonawca udzieli gwarancji na prawidłowe działanie wykonanej konfiguracji na okres nie krótszy niż **24** miesięcy od dnia odbioru wdrożenia w danej sieci.

7. Terminy realizacji i odbiór

7.1. Termin dostawy licencji, aktywacji wsparcia producenta i przekazania vouchera szkoleniowego: do 20 dni od dnia zawarcia umowy.

7.2. Termin realizacji wdrożenia: do **14** dni.

7.3. Odbiór licencji nastąpi na podstawie protokołu odbioru, po przekazaniu dokumentów licencyjnych dla obu instancji, potwierdzenia rejestracji wsparcia producenta oraz vouchera szkoleniowego.

7.4. Odbiór wdrożenia nastąpi odrębnie dla sieci IT i dla sieci OT, na podstawie protokołów odbioru podpisanych po pozytywnym wyniku testów z pkt 6.3.9 oraz przekazaniu dokumentacji z pkt 6.3.10. Po odbiorze wdrożenia w obu sieciach strony podpiszą protokół odbioru końcowego.

8. Rozwiązania równoważne

8.1. Wskazanie w OPZ nazw systemów, z którymi oferowane oprogramowanie musi się integrować (m.in. RTIR, Jira, Office 365 / Microsoft Exchange, Slack, Microsoft Teams, Mattermost, Energy Logserver, MISP), wynika z infrastruktury i narzędzi wykorzystywanych przez Zamawiającego i nie stanowi wskazania oferowanego produktu.

8.2. Pozostałe nazwy własne, znaki towarowe lub normy wskazane w OPZ mają charakter przykładowy. Zamawiający dopuszcza rozwiązania równoważne, zgodnie z art. 99 ust. 5 i art. 101 ust. 4 ustawy Prawo zamówień publicznych. Wykonawca, który powołuje się na rozwiązanie równoważne, jest obowiązany wykazać, że oferowane rozwiązanie spełnia wymagania określone przez Zamawiającego.