

## OPIS PRZEDMIOTU ZAMÓWIENIA

Przedmiotem zamówienia jest dostawa i wdrożenie zintegrowanego systemu klasy SOAR (Security Orchestration, Automation and Response)

Realizacja przedmiotu zamówienia polega na dostarczeniu i wdrożeniu rozwiązania typu SOAR (Security Orchestration, Automation and Response), zwanego dalej „Systemem SOAR”, w ramach którego wykonawca zrealizuje:

- **Dostawę oprogramowania klasy SOAR** wraz z wymaganymi licencjami dla **6 operatorów SOC**, w tym co najmniej **2 użytkowników o uprawnieniach administracyjnych**, z zapewnieniem **36-miesięcznego wsparcia producenta**, rozliczanego w cyklach rocznych;
- **Dostawę niezbędnego sprzętu**, zgodnego z wymaganiami technicznymi i wydajnościowymi niezbędnymi do prawidłowego działania Systemu SOAR;
- **Wdrożenie i konfigurację Systemu**, obejmującą jego dostosowanie do wymagań Zamawiającego oraz **integrację z posiadanymi przez Zamawiającego systemami bezpieczeństwa** (takimi jak: SIEM, EDR, NDR, WAF, FW, IAM, IOC, itp.);
- **Świadczenie usługi gwarancji i wsparcia technicznego** dla wdrożonego Systemu przez okres **36 miesięcy**, zgodnie z wymaganym poziomem SLA oraz zakresem usług utrzymaniowych i serwisowych;
- **Przeprowadzenie instruktażu (warsztatów)** dla użytkowników i administratorów Systemu SOAR, umożliwiające jego samodzielne użytkowanie, konfigurację i rozwój.

Realizacja przedmiotu Umowy obejmuje wykonanie ośmiu zadań:

Zadanie I – Opracowanie projektu technicznego Systemu SOAR

Zadanie II – Dostawa Systemu SOAR

Zadanie III – Wdrożenie Systemu SOAR

Zadanie IV – Integracja Systemu SOAR z posiadanymi systemami bezpieczeństwa

Zadanie V – Optymalizacja działania Systemu SOAR

Zadanie VI – Opracowanie dokumentacji powykonawczej Systemu SOAR

Zadanie VII – Przeprowadzenie instruktażu (warsztatów)

Zadanie VIII – Świadczenie gwarancji i wsparcia technicznego

## DEFINICJE

Na potrzeby niniejszego dokumentu, określenia poniższe będą miały następujące znaczenie:

Termin	Definicja
<b>Alert Bezpieczeństwa</b>	Zdarzenie lub grupa zdarzeń, sklasyfikowanych przez systemy bezpieczeństwa (np. SIEM, EDR) jako potencjalne zagrożenie. Powstaje w wyniku korelacji zdarzeń i stanowi punkt wyjścia do analizy prowadzonej przez zespół SOC.
<b>Aktualizacje</b>	Uaktualnienia oprogramowania dostarczane w ramach Wsparcia Technicznego, obejmujące m.in. nowe wersje, poprawki, patche oraz inne zmiany mające na celu zapewnienie prawidłowego działania systemu.
<b>Automatyzacja</b>	Proces konfiguracji systemu SOAR do samodzielnego wykonywania zadań lub sekwencji działań w odpowiedzi na zdefiniowane wyzwalacze (np. alerty, incydenty), bez lub przy minimalnym udziale człowieka.
<b>Awaria</b>	Nieprawidłowe działanie urządzeń lub oprogramowania, uniemożliwiające ich wykorzystanie zgodnie z przeznaczeniem lub dokumentacją producenta.
<b>BYOI (Bring Your Own Integration)</b>	Mechanizm umożliwiający użytkownikowi systemu SOAR samodzielne tworzenie, modyfikację i wdrażanie integracji z systemami bezpieczeństwa poprzez skrypty (np. Python, PowerShell) lub dedykowane narzędzia, bez konieczności angażowania producenta.
<b>Czas Naprawy</b>	Okres od momentu zgłoszenia awarii do chwili przywrócenia pełnej funkcjonalności i efektywności działania urządzenia lub systemu.
<b>Czas Reakcji</b>	Maksymalny dopuszczalny czas od chwili zgłoszenia awarii do potwierdzenia przez serwis Wykonawcy przyjęcia zgłoszenia do realizacji.
<b>CTI (Cyber Threat Intelligence)</b>	Informacje o zagrożeniach cybernetycznych, obejmujące techniki ataków, wskaźniki kompromitacji (IOC), taktyki i procedury (TTP), a także dane o aktorach zagrożeń, wykorzystywane do proaktywnego zarządzania ryzykiem.
<b>Dokumentacja</b>	Dokumenty przygotowane przez Wykonawcę w języku polskim, przekazane Zamawiającemu w ramach realizacji umowy. Dokumentacja ma formę elektroniczną i wymaga zatwierdzenia przez Zamawiającego.
<b>Incydent Bezpieczeństwa</b>	Zdarzenie lub zbiór zdarzeń potwierdzających naruszenie polityki bezpieczeństwa lub zabezpieczeń, wymagające formalnej reakcji zgodnie z procedurami, uruchamiającej odpowiednie działania (np. playbooki, eskalację, dokumentację).
<b>Integracja</b>	Proces połączenia systemów w celu umożliwienia komunikacji i wymiany danych; może mieć formę natywną (wbudowaną) lub własną (BYOI).
<b>Integracja Dwukierunkowa</b>	Integracja umożliwiająca wymianę danych i wzajemne wywoływanie działań pomiędzy systemami (np. SOAR pobiera alerty z SIEM i odsyła status incydentu).
<b>IOC (Indicators of Compromise)</b>	Artefakty (np. adresy IP, domeny, skróty plików) wskazujące na naruszenie bezpieczeństwa.
<b>MTTD (Mean Time To Detect)</b>	Średni czas potrzebny na wykrycie incydentu bezpieczeństwa od momentu jego wystąpienia.
<b>MTTR (Mean Time To Respond/Resolve)</b>	Średni czas potrzebny na reakcję oraz pełne rozwiązanie incydentu bezpieczeństwa.
<b>Orkiestracja Bezpieczeństwa</b>	Koordinacja i automatyzacja działań różnych narzędzi i systemów bezpieczeństwa w celu efektywnego zarządzania incydentami.
<b>Playbook</b>	Gotowy scenariusz automatycznej reakcji na incydent bezpieczeństwa, zawierający ścieżki decyzyjne, zadania manualne i automatyczne oraz integracje z zewnętrznymi narzędziami.
<b>RBAC (Role-Based Access Control)</b>	Mechanizm kontroli dostępu oparty na rolach, umożliwiający przypisywanie uprawnień do funkcji systemu w zależności od roli użytkownika.
<b>RCA (Root Cause Analysis)</b>	Analiza przyczyn podstawowych incydentu lub awarii, mająca na celu identyfikację źródłowego błędu lub słabości w systemie, w celu zapobieżenia jego ponownemu wystąpieniu.
<b>Scenariusz</b>	Logika działania systemu SOAR, zawierająca działania ręczne, automatyczne, warunkowe oraz podscenariusze.
<b>System SOAR</b>	Kompleksowe, zaawansowane rozwiązanie technologiczne, obejmujące oprogramowanie, sprzęt, licencje, integracje oraz dokumentację, służące do automatyzacji, orkiestracji i skutecznego zarządzania incydentami bezpieczeństwa.

<b>SIEM (Security Information and Event Management)</b>	System do centralnego zbierania, korelowania i analizy logów oraz zdarzeń bezpieczeństwa z różnych źródeł, służący do wykrywania zagrożeń i generowania alertów.
<b>SLA (Service Level Agreement)</b>	Umowa o gwarantowanym poziomie usług, określająca m.in. czasy reakcji, czasy naprawy i inne metryki jakościowe.
<b>SOC (Security Operations Center)</b>	Zespół, infrastruktura i procesy odpowiedzialne za monitorowanie, analizę i reagowanie na incydenty bezpieczeństwa.
<b>TIP (Threat Intelligence Platform)</b>	Platforma do gromadzenia, analizy i dystrybucji informacji o zagrożeniach (CTI), w tym IOC i IOA.
<b>Urządzenia</b>	Sprzęt wraz z wyposażeniem oraz dokumentacją techniczną producenta.
<b>Workflow</b>	Sekwencja kroków niezbędnych do realizacji określonego procesu, np. obsługi incydentu w systemie SOAR.
<b>Wskaźnik (Indicator)</b>	Dowód analityczny wskazujący na potencjalną złośliwą aktywność (np. adres IP, URL, skrót pliku).
<b>Asysta techniczna Wykonawcy</b>	Usługi świadczone przez Wykonawcę w zakresie pomocy technicznej, obejmujące diagnozowanie i usuwanie problemów, reagowanie na awarie, wsparcie konfiguracyjne oraz współpracę z producentem w razie potrzeby.
<b>Wsparcie producenta</b>	Usługi świadczone przez producenta systemu, obejmujące dostęp do aktualizacji, poprawek, dokumentacji, baz wiedzy oraz pomoc techniczną w okresie ważności licencji.
<b>Zdarzenie Bezpieczeństwa</b>	Zdarzenie w systemie informatycznym lub sieci mogące mieć znaczenie dla bezpieczeństwa (np. nieudane logowanie, uruchomienie nieznanego programu).

Pozostałe pojęcia użyte w dokumencie należy rozumieć zgodnie z ich ogólnie przyjętym znaczeniem.

## 1. WYMAGANIA OGÓLNE DLA SYSTEMU SOAR

Oferowany system musi spełniać następujące wymagania:

- 1.1. Być systemem klasy SOAR (Security Orchestration, Automation and Response).
- 1.2. Pochodzić od jednego producenta i stanowić jednolity, w pełni zintegrowany system, obejmujący co najmniej następujące funkcje zgodne z definicją Gartnera:
  - a) orkiestrację i automatyzację działań związanych z bezpieczeństwem (SOA),
  - b) zarządzanie reakcją na incydenty bezpieczeństwa (SIR),
  - c) przetwarzanie i analizę informacji o zagrożeniach (TIP).

- 1.3. Być wdrożony lokalnie (on-premise) na dedykowanej fizycznej platformie serwerowej dostarczonej przez Wykonawcę.

Dopuszcza się zastosowanie hypervisorów (np. VMware ESX) na klastrze utworzonym z dostarczonego sprzętu w celu zapewnienia wysokiej dostępności (HA), pod warunkiem, że cała infrastruktura – zarówno sprzętowa, jak i wirtualna – zostanie dostarczona i wdrożona przez Wykonawcę jako integralna część systemu. W przypadku zastosowania hypervisorów Wykonawca zobowiązany jest również do dostarczenia bezterminowych licencji Veeam Backup & Replication w modelu „per procesor” (Processor License), obejmujących wszystkie gniazda procesorów we wszystkich serwerach fizycznych tworzących klastr, wraz z 36-miesięcznym wsparciem producenta (Basic Support). Licencje muszą umożliwiać pełną integrację z systemem SOAR i realizację polityki kopii zapasowych Zamawiającego.

- 1.4. Umożliwiać szczegółowe logowanie (granularne audytowanie) działań użytkowników systemu. Logowaniu powinny podlegać co najmniej:
  - a) logowanie użytkowników do systemu,
  - b) tworzenie, edycja i usuwanie playbooków, skryptów oraz innych obiektów,
  - c) instalacja nowych integracji,
  - d) zmiany w konfiguracji systemu
  - e) zmian w uprawnieniach użytkowników.
- 1.5. System musi zapewniać integralność logów audytowych (np. podpis cyfrowy, tryb tylko do odczytu, repozytorium WORM) oraz możliwość ich przesyłania w czasie rzeczywistym do zewnętrznego systemu logowania (SIEM) z wykorzystaniem standardowych protokołów (Syslog, REST API lub równoważnych). Dostęp do logów musi być ograniczony i kontrolowany, a wszystkie próby ich odczytu, eksportu lub zmiany rejestrowane i przekazywane do SIEM.
- 1.6. System musi wspierać szyfrowanie danych w spoczynku i transmisji, MFA, kontrolę dostępu opartą na rolach oraz integrację z mechanizmami SSO.

## 2. WYMAGANIA FUNKCJONALNE

### 2.1. Zarządzanie incydentami i automatyzacja

System SOAR musi zapewniać kompleksowe zarządzanie incydentami bezpieczeństwa oraz wspierać ich automatyczną analizę, klasyfikację, obsługę i dokumentowanie.

#### 2.1.1. Obsługa komunikacji i współpracy

- a) System musi umożliwiać dwustronną komunikację zarówno z użytkownikami systemu (np. w celu zebrania dodatkowych informacji), jak i pomiędzy operatorami SOC, z wykorzystaniem interaktywnych formularzy.
- b) Musi wspierać delegowanie zadań członkom zespołu SOC w ramach obsługi danego incydentu.

Formularze muszą:

- a) Być edytowalne przez administratora systemu bez konieczności programowania,
- b) Umożliwiać różne typy pól (tekstowe, listy, pola wyboru, daty),
- c) Obsługiwać warunkowe wyświetlanie pól,
- d) Być zapisywane w historii incydentu,
- e) Mogą wpływać na dalszy przebieg scenariusza (np. jako warunek w zadaniu ręcznym).

Komunikacja musi być możliwa przez co najmniej następujące kanały:

- a) Wewnętrzny interfejs graficzny (GUI),
- b) E-mail,
- c) Integrację z komunikatorami (np. Microsoft Teams, Slack),
- d) API lub webhooks do zewnętrznych systemów (np. SerwisDesk).

#### 2.1.2. Typy i parametryzacja incydentów

- a) System musi posiadać wbudowaną bibliotekę co najmniej 20 predefiniowanych typów incydentów, w tym typów powiązanych z integrowanymi systemami (np. phishing, malware, DDoS, nieuprawniony dostęp, atak na systemy wewnętrzne, inne typowe przypadki związane z integrowanymi systemami bezpieczeństwa).
- b) Alternatywnie dopuszcza się system zawierający mniej niż 20 gotowych typów, o ile spełnia on wszystkie poniższe warunki:
  - Możliwość tworzenia dowolnej liczby własnych typów incydentów,
  - Tworzenie i edycja typów możliwa jest przez administratora systemu (Zamawiającego) bez konieczności:
    - pisania kodu (skryptów),
    - angażowania Wykonawcy,
    - ponoszenia dodatkowych kosztów.
  - Czas utworzenia nowego typu incydentu nie przekracza 30 minut dla użytkownika z podstawową wiedzą o systemie.
  - Zmiany nie wymagają restartu systemu ani nie wpływają na jego dostępność.
- c) System musi umożliwiać tworzenie i edycję własnych:
  - typów incydentów,
  - pól i etykiet incydentów,
  - typów i pól wskaźników (IoC),
  - raportów,
  - dashboardów.

Wszystkie powyższe elementy muszą być tworzone i modyfikowane przez administratora systemu za pomocą interfejsu graficznego, bez konieczności programowania.

#### 2.1.3. Automatyzacja rejestracji i wypełniania incydentów

- a) System musi umożliwiać automatyczne generowanie karty incydentu.
- b) Musi wspierać automatyczne uzupełnianie pól incydentu na podstawie jego typu lub atrybutów.

#### 2.1.4. Dokumentowanie działań i historia incydentu

System musi umożliwiać kompleksowe dokumentowanie i przechowywanie historii obsługi incydentu, w sposób umożliwiający jej wykorzystanie do celów audytowych, szkoleń, transferu wiedzy oraz dochodzeń.

Historia musi zawierać:

- a) wprowadzone zmiany,
- b) osoby zaangażowane w obsługę,
- c) wydane komendy i ich wyniki,
- d) wykonane zadania z playbooków i ich rezultaty,
- e) wyniki działań automatycznych i ręcznych,
- f) komentarze analityków,
- g) wyniki komend CLI wykonywanych przez operatorów,
- h) wskaźniki zagrożeń (IoC) – zarówno wyodrębnione automatycznie, jak i dodane ręcznie,
- i) dowody wskazane przez analityków (np. zrzuty ekranu, próbki plików),
- j) pliki dodane do historii obsługi.

Materiał dowodowy (w tym pliki, zrzuty, próbki) musi być przechowywany w sposób chroniący przed przypadkową lub nieuprawnioną modyfikacją, usunięciem lub nadpisaniem.

System musi ponadto:

- a) zapewniać możliwość eksportu kompletnego materiału dowodowego w formacie zapewniającym integralność (np. z podpisem cyfrowym),
- b) rejestrować wszystkie próby dostępu, eksportu lub modyfikacji materiału dowodowego,
- c) zapewniać zgodność z wymogiem przechowywania danych przez min. 730 dni (pkt 3.1.1b).

#### 2.1.5. Dokumentowanie działań w ramach incydentu

System musi umożliwiać dokumentowanie następujących informacji związanych z obsługą incydentu:

- a) wprowadzonych zmian,
- b) osób zaangażowanych w obsługę,
- c) wydanych komend i ich wyników,
- d) wykonanych zadań z playbooków i ich rezultatów.

#### 2.1.6. Historia incydentu i transfer wiedzy

System musi umożliwiać zapisywanie historii obsługi incydentu w sposób umożliwiający wykorzystanie jej do celów szkoleniowych i transferu wiedzy. Historia powinna zawierać:

- a) wyniki działań automatycznych i ręcznych,
- b) komentarze analityków,
- c) wyniki komend CLI wykonywanych przez operatorów,
- d) wskaźniki zagrożeń (IoC) – zarówno wyodrębnione automatycznie, jak i dodane ręcznie,
- e) dowody wskazane przez analityków (np. zrzuty ekranu, próbki plików),
- f) pliki dodane do historii obsługi.

#### 2.1.7. Obsługa reguł wstępnego przetwarzania

System musi umożliwiać definiowanie reguł wstępnego przetwarzania (pre-process rules), służących m.in. do deduplikacji, zamykania lub odrzucania nowo zgłoszonych incydentów, jeszcze przed rozpoczęciem ich obsługi.

#### 2.1.8. Monitorowanie statusu incydentów

System musi umożliwiać identyfikację incydentów, które pozostają nieobsłużone.

#### 2.1.9. Automatyzacja działań i ręczne uruchamianie zadań

- a) System musi automatyzować analizę danych, przekazywanie informacji oraz podejmowanie działań naprawczych.
- b) Operator SOC musi mieć możliwość doraźnego uruchamiania pojedynczych akcji automatyzacyjnych (integracyjnych, analitycznych, śledczych) bezpośrednio z interfejsu graficznego (GUI), bez konieczności tworzenia ani modyfikacji playbooków.
- c) Podczas uruchamiania akcji operator musi mieć możliwość wprowadzenia parametrów wejściowych (np. adres IP, hash pliku, nazwa użytkownika).
- d) Akcje uruchamiane w kontekście incydentu muszą być automatycznie zapisywane w jego historii.

#### 2.2. Playbooki i scenariusze automatyzacji

System SOAR powinien wspierać tworzenie, uruchamianie i zarządzanie graficznymi scenariuszami automatyzacji (playbookami), w tym:

##### 2.2.1. Gotowe i własne scenariusze

- a) System musi zapewniać co najmniej 10 prekonfigurowanych scenariuszy obejmujących kluczowe przypadki użycia, takie jak: analiza phishingu, izolacja hosta, blokada adresu IP, wzbogacenie danych o reputację (IoC), eskalacja incydentu do CISO.
- b) System musi umożliwiać kopiowanie, edytowanie i tworzenie nowych scenariuszy, również w oparciu o gotowe szablony.
- c) Graficzny edytor scenariuszy musi umożliwiać: dodawanie zadań (ręcznych i automatycznych), definiowanie warunków decyzyjnych, integrację z systemami zewnętrznymi, tworzenie formularzy interaktywnych – bez konieczności pisania kodu.
- d) Zmiany wymagające zaawansowanej logiki (np. filtrowanie danych, transformacja struktur) mogą wykorzystywać wbudowane edytory skryptowe (np. Python, PowerShell).

##### 2.2.2. Funkcjonalność scenariuszy

System powinien umożliwiać:

- a) definiowanie zadań ręcznych i automatycznych,
- b) obsługę zadań warunkowych, akwizycję danych poprzez interaktywne formularze, które:
  - mogą być edytowane przez administratora bez kodowania,
  - obsługują różne typy pól (tekst, listy rozwijane, checkboxy, daty, adresy IP),
  - umożliwiają warunkowe wyświetlanie pól,
  - są zapisywane w historii incydentu,
  - mogą wpływać na przebieg scenariusza,
- c) stosowanie filtrów danych, wykorzystywanie scenariuszy zagnieżdżonych (podscenariuszy), z możliwością ich ponownego użycia i automatycznego dziedziczenia zmian.

System musi dodatkowo zapewniać:

- wersjonowanie playbooków i podscenariuszy, z możliwością porównywania, przywracania i audytowania zmian,
- modyfikowanie lub dodawanie zadań w trakcie wykonywania scenariusza, bez konieczności restartu i przy zachowaniu integralności historii.

##### 2.2.3. Uruchamianie i sterowanie scenariuszami

System musi umożliwiać elastyczne uruchamianie i kontrolę scenariuszy w różnych trybach:

- a) Automatyczne uruchamianie na podstawie: nowo zgłoszonych incydentów, wybranych typów incydentów, wskaźników kompromitacji (IoC), wyników analizy kontekstowej (np. reputacja IP, typ pliku) oraz wyzwalaczy zewnętrznych (np. SIEM, EDR, WAF).



- b) Ręczne uruchamianie z GUI, w kontekście bieżącego incydentu, z możliwością podania parametrów wejściowych (np. adres IP, hash pliku, użytkownik).
- c) Uruchamianie w trybie krokowym (debug), umożliwiającym analizę przebiegu, weryfikację wyników i identyfikację błędów, bez wpływu na system produkcyjny (np. w trybie testowym/symulacyjnym).
- d) Ponowne uruchamianie scenariuszy dla wybranych incydentów, z możliwością wznowienia od dowolnego etapu, powtórzenia pojedynczych zadań oraz zachowania historii poprzednich uruchomień.
- e) Uruchamianie okresowe według harmonogramu, np. do monitorowania stanu systemów, aktualizacji danych (IOC) lub realizacji playbooków typu threat hunting.
- f) Wyzwalanie scenariuszy na podstawie wskaźników kompromitacji (IOC) wskazanych przez użytkownika, w tym automatyczne playbooksi typu threat hunting.
- g) Możliwość przerywania lub zatrzymania uruchomionego scenariusza przez uprawnionego użytkownika, z rejestrowaniem tej czynności w logach audytowych.

#### 2.2.4. Interakcja z użytkownikiem

System musi umożliwiać elastyczną i bezpieczną interakcję z użytkownikami, zarówno w ramach obsługi incydentów, jak i zarządzania zadaniami w zespole SOC.

- a) Sterowanie przebiegiem scenariusza przez analityka, w szczególności w zadaniach warunkowych ręcznych (np. potwierdzenie izolacji hosta, ocena priorytetu incydentu).
- b) Przydzielanie zadań do członków zespołu SOC, w tym:
  - przypisanie zadania do użytkownika,
  - ustalenie terminu realizacji,
  - eskalację zadania.
- c) Modyfikowanie lub dodawanie zadań w trakcie wykonywania scenariusza, przy czym:
  - zmiany nie mogą naruszać integralności historii,
  - nowe zadania są zapisywane w historii incydentu,
  - wszystkie zmiany są rejestrowane w logach audytowych.
- d) Przekazywanie parametrów pomiędzy zadaniami oraz odczytywanie wyników z podscenariuszy, w tym:
  - wykorzystanie danych wyjściowych jednego zadania jako danych wejściowych kolejnego,
  - dostęp do wyników zadań warunkowych i ręcznych,
  - obsługę zmiennych globalnych i lokalnych.
- e) Obsługę interaktywnych formularzy, które:
  - są edytowalne bez konieczności pisania kodu,
  - obsługują różne typy pól (tekst, listy, pola wyboru, daty, adresy IP),
  - umożliwiają warunkowe wyświetlanie pól,
  - są zapisywane w historii incydentu,
  - mogą wpływać na przebieg scenariusza (np. jako warunek w zadaniu ręcznym).

#### 2.2.5. Monitoring i dokumentowanie

System powinien:

- a) dokumentować przebieg wykonania scenariusza wraz z rezultatami poszczególnych zadań,
- b) umożliwiać wizualizację przebiegu wykonania (z podziałem na wykonane, pominięte i warunkowe zadania),
- c) umożliwiać bieżące monitorowanie stanu wykonania scenariusza powiązanego z incydemtem,
- d) informować odpowiednie osoby w przypadku wystąpienia anomalii podczas jego realizacji,
- e) udostępniać historię uruchomień scenariuszy i wykonanych zadań.

#### 2.2.6. Rozszerzalność



System powinien umożliwiać rozszerzenie funkcjonalności poprzez własne skrypty, m.in. do:

- a) realizacji niestandardowych operacji warunkowych i filtracji danych,
- b) modyfikacji i prezentacji danych w dashboardach,
- c) uruchamiania zadań po zakończeniu obsługi incydentu.

Skrypty muszą być kompatybilne z formatami wspieranymi przez system (np. .py, .js, .ps1) i mogą wykorzystywać wbudowane edytory lub zewnętrzne środowiska programistyczne.

#### 2.2.7. Obsługa języków skryptowych

System musi zapewniać obsługę języków skryptowych (co najmniej Python, JavaScript, PowerShell) do automatyzacji zadań oraz tworzenia własnych playbooków i integracji. System może również wspierać dodatkowe języki skryptowe (np. Bash, Ruby), o ile są one kompatybilne z architekturą platformy.

#### 2.2.8. Wykorzystanie zewnętrznych bibliotek

System musi umożliwiać wykorzystanie w skryptach zewnętrznych bibliotek oraz programów, np. poprzez uruchamianie skryptów w kontenerze z wymaganym oprogramowaniem.

Obsługa kontenerów opartych na Docker jest wymagana. Obsługa orchestratorów (np. Kubernetes) jest opcjonalna.

Kontenery muszą zapewniać izolację na poziomie:

- procesów,
- przestrzeni sieciowej,
- systemu plików,
- uprawnień dostępu.

Mechanizmy izolacji muszą zapobiegać wyciekowi danych i nieuprawnionemu dostępowi do zasobów systemu SOAR.

#### 2.2.9. Integracja z narzędziami developerskimi

System powinien umożliwiać integrację z popularnymi środowiskami programistycznymi typu IDE (np. Visual Studio Code) w celu edycji i debugowania skryptów. Integracja może być zrealizowana na etapie wdrożenia. Zamawiający dopuszcza użycie SDK lub API.

Dopuszcza się, że SDK lub API wymaga dodatkowego wdrożenia lub konfiguracji, o ile nie blokuje to podstawowych funkcjonalności systemu ani nie wydłuża harmonogramu wdrożenia.

Wykonawca zobowiązuje się do zapewnienia pełnej dokumentacji integracji oraz wsparcia technicznego w jej zakresie.

#### 2.2.10. System SOAR powinien wspierać integrację z frameworkiem MITRE ATT&CK w zakresie:

- a) Mapowanie playbooków do taktyk i technik MITRE ATT&CK – każdy playbook może być przypisany do jednej lub wielu technik,
- b) Wyszukiwanie i filtrowanie playbooków na podstawie taktyk lub technik MITRE,
- c) Automatyczne wyzwalanie playbooków na podstawie identyfikacji technik MITRE w alertach z SIEM lub EDR,
- d) Integracja z bazą wiedzy MITRE ATT&CK (online lub z aktualizowaną lokalną kopią),
- e) Eksport mapowania playbooków do technik MITRE w formacie CSV lub JSON,
- f) Wspieranie scenariuszy threat hunting opartych na TTP, w tym uruchamianie playbooków typu „hunt for T1003 – OS Credential Dumping”.

### 2.3. Integracje i Threat Intelligence

#### 2.3.1. Integracje z systemami bezpieczeństwa, SIEM i środowiskiem SOC

System SOAR musi zapewniać elastyczną i bezpieczną integrację z systemami bezpieczeństwa, SIEM oraz infrastrukturą SOC, zgodnie z wymogami operacyjnymi i zabezpieczeniowymi:

- a) System musi umożliwiać integrację z co najmniej następującymi kategoriami systemów:
  - SIEM (Energy Logserver – obowiązkowa, natywna lub funkcjonalna integracja),
  - EPP/EDR (np. McAfee, Symantec, TrendMicro, CrowdStrike),
  - Active Directory (zarządzanie użytkownikami, synchronizacja grup),
  - Firewall/NGFW (Check Point, Palo Alto, Fortinet),
  - Web Application Firewall (WAF),
  - Systemy E-mail i komunikacyjne (np. Microsoft 365, serwery pocztowe),
  - Skanery podatności (np. Nessus, Qualys),
  - Systemy ticketowe (np. SerwisDesk),
  - Repozytoria Threat Intelligence (np. VirusTotal, MISP, IBM X-Force).
- b) System musi wspierać mechanizmy BYOI (Bring Your Own Integration), umożliwiające rozbudowę liczby integracji poza gotowe konektory, w tym:
  - możliwość klonowania i modyfikacji istniejących integracji,
  - dostęp do dokumentacji API i przykładów kodu,
  - narzędzia do debugowania i testowania nowych integracji.Dopuszcza się ograniczenia funkcjonalne, o ile nie uniemożliwiają realizacji kluczowych scenariuszy automatyzacji.
- c) Integracje mogą wymagać podstawowej wiedzy programistycznej (np. Python, PowerShell) do tworzenia i modyfikacji skryptów, ale nie mogą wymagać angażowania producenta ani dodatkowych kosztów.
- d) System musi obsługiwać wiele instancji integracji tego samego typu (np. więcej niż jeden system EDR lub firewall).
- e) System musi wspierać integrację z systemem SIEM oraz środowiskiem SOC w zakresie:
  - odbierania zdarzeń i alertów bezpieczeństwa,
  - przekazywania poleceń reakcji i eskalacji (np. blokada IP, izolacja hosta),
  - aktualizacji statusów incydentów,
  - synchronizacji metadanych i danych kontekstowych (np. właściciela, priorytetu).
- f) Integracja musi być realizowana za pomocą konektora, API, webhooka, kolejek komunikatowych (np. Kafka, RabbitMQ) lub innych wspieranych mechanizmów, z możliwością wyboru:
  - synchronicznej komunikacji (np. REST API) – dla akcji wymagających natychmiastowej odpowiedzi,
  - asynchronicznej komunikacji (np. kolejki, pliki) – dla masowego przesyłania danych.
- g) Dla każdej integracji Wykonawca przekaze dokumentację zawierającą:
  - sposób działania i zakres wymiany danych,
  - protokoły i metody uwierzytelniania (np. API key, tokeny, certyfikaty),
  - wymagania techniczne (IP, porty, firewall),
  - schematy danych i mapowanie pól,
  - procedury obsługi błędów i monitorowania.

### 2.3.2. Integracje z CTI (Cyber Threat Intelligence)

System SOAR musi wspierać integrację z zewnętrznymi źródłami informacji o zagrożeniach, umożliwiając automatyczne wzbogacanie danych i reakcję na nowe zagrożenia, w tym:

- a) pobieranie informacji o zagrożeniach (np. adresy IP, domeny, skróty plików) z różnych źródeł CTI,

- b) wykorzystanie zewnętrznych baz CTI w przypadku braku natywnej bazy producenta (np. MISP, VirusTotal, IBM X-Force),
- c) obsługę formatów:
  - strukturalnych: JSON, CSV, STIX 1.x/2.x,
  - niestukturalnych: e-mail, wiadomości, kanały RSS,
- d) realizację funkcji:
  - subskrypcji zewnętrznych i wewnętrznych feedów CTI,
  - automatycznego aktualizowania list IoC,
  - generowania powiadomień o nowych lub podejrzanych wskaźnikach (np. w GUI, e-mail, komunikator),

### 2.3.3. Wskaźniki zagrożeń (Indicators)

System SOAR musi zapewniać zaawansowane zarządzanie wskaźnikami kompromitacji, w tym ich gromadzenie, wzbogacanie, wersjonowanie i dezaktywację.

- a) System musi posiadać centralne repozytorium wskaźników, gromadzące i korelujące dane z:
  - incydentów,
  - alertów,
  - zewnętrznych feedów CTI.
- b) System musi wspierać co najmniej następujące typy wskaźników:
  - adres email,
  - konto użytkownika,
  - CVE,
  - domena, FQDN, hostname,
  - adresy IP (v4 i v6), CIDR,
  - URL,
  - klucz i ścieżka rejestru (opcjonalnie),
  - możliwość własnej definicji wskaźników, ich pól i skryptów reputacyjnych;
- c) System musi umożliwiać własne definiowanie typów wskaźników, ich pól i skryptów reputacyjnych.
- d) System musi zapewniać automatyczne wzbogacanie wskaźników (enrichment) z wykorzystaniem zewnętrznych źródeł (np. reputacja IP, historia domeny).
- e) System musi umożliwiać uruchamianie odpowiednich scenariuszy (playbooków) na podstawie typu lub reputacji wskaźnika, np:
  - playbook „Threat Hunting” dla nowego IOC,
  - playbook „Izolacja hosta” dla IOC z reputacją „malicious”.
- f) System musi zapewniać wersjonowanie list IOC, z możliwością:
  - porównywania zmian,
  - przywracania poprzednich wersji,
  - śledzenia, kto i kiedy dodał/usunął wskaźnik.
- g) System musi wspierać automatyczne dezaktywowanie lub wycofywanie :
  - po upływie określonego czasu życia (TTL),
  - na podstawie reguł (np. IOC uznany za fałszywy po analizie),
  - po ręcznym oznaczeniu jako „false positive”.
- h) W przypadku braku natywnej funkcjonalności, dopuszcza się realizację powyższych mechanizmów za pomocą playbooków lub skryptów.

### 2.3.4. Artefakty incydentu

System SOAR musi umożliwiać ustrukturyzowane definiowanie artefaktów incydentu, obejmujących co najmniej:

- pliki i ich skróty (SHA1, SHA256, MD5),
- adresy IP i URL,
- DNS, Hostname, Port,
- użytkownik, adres email,
- rejestr i proces (opcjonalnie).

## 2.4. Raportowanie i wizualizacja

System SOAR musi umożliwiać tworzenie, prezentację oraz eksport raportów i dashboardów w celu monitorowania kondycji SOC, incydentów oraz działań operacyjnych.

### 2.4.1. Gotowe i własne raporty

- a) System powinien zawierać zestaw gotowych raportów, w tym:
  - Raport dzienny oraz 7-dniowy i 30-dniowy dotyczący incydentów,
  - raport średniego czasu obsługi/rozwiązania incydentów (MTTR),
  - raport podsumowania zmiany SOC,
  - raport otwartych i opóźnionych incydentów.
- b) W przypadku braku wskazanych raportów system musi umożliwiać ich utworzenie wewnętrznie lub poprzez integrację z zewnętrznymi narzędziami raportowymi (np. Kibana).
- c) System musi umożliwiać tworzenie własnych raportów oraz kart incydentów, z możliwością:
  - dostosowania zawartości przy użyciu pól z incydentów oraz pól własnych,
  - dodawania tekstu opisowego i komentarzy,
  - stosowania filtrów, grupowania i agregacji danych.
- d) System musi umożliwiać generowanie raportów dla różnych poziomów odbiorców w organizacji, w szczególności:
  - poziom strategiczny (np. CISO, kierownictwo),
  - poziom operacyjny (np. SOC manager, koordynator zespołu),
  - poziom analityczny (analitycy bezpieczeństwa).
- e) System musi umożliwiać raportowanie wskaźników SLA i KPI związanych z obsługą incydentów, w tym terminowości i efektywności działań.
- f) System powinien umożliwiać raportowanie korzyści wynikających z automatyzacji i orkiestracji, w tym oszczędności czasu, zasobów, kosztów oraz liczby zagrożeń, którym udało się zapobiec.

### 2.4.2. Tworzenie i personalizacja dashboardów

- a) System musi umożliwiać tworzenie własnych dashboardów z wykorzystaniem predefiniowanych komponentów wizualnych (np. wykresy kołowe, słupkowe, liniowe, tabele, mapy cieplne).
- b) Dashboardy powinny umożliwiać prezentację m.in.:
  - kondycji SOC i powiązanego ryzyka biznesowego (np. MTTD/MTTR),
  - produktywności członków zespołu SOC,
  - liczby i statusu incydentów (np. właściciel, typ, czas rozwiązania),
  - kondycji systemu SOAR (np. zużycie zasobów, pamięci, CPU).
  - aktywności playbooków (liczba uruchomień, sukcesów, błędów).
- c) System musi umożliwiać udostępnianie dashboardów dla określonych ról lub użytkowników.

### 2.4.3. Wyszukiwanie i powiązania incydentów

System SOAR musi:

- zapewniać intuicyjny interfejs graficzny umożliwiający szybkie wyszukiwanie incydentów po atrybutach, wspierany przez zaawansowany język zapytań do filtrowania i analizy danych
- umożliwiać identyfikację i wizualizację incydentów powiązanych na podstawie wspólnych wskaźników zagrożeń (IoC), assetów, źródeł lub celów ataku,
- wspierać graficzną analizę powiązań między incydentami, wskaźnikami i innymi obiektami (assetami, podatnościami, alarmami, hostami, użytkownikami), prezentowaną w sposób przejrzysty i ułatwiający interpretację.

#### 2.4.4. Eksport danych i wyróżnianie informacji

- a) System musi umożliwiać oznaczanie kluczowych informacji o incydencie (np. główny IoC, krytyczny host, osoba odpowiedzialna) w celu ich wyróżnienia w interfejsie oraz w raportach. Wyróżnienia mogą obejmować tagi, kolory, priorytety lub flagi i muszą być widoczne w przeglądzie incydentu, dashboardach oraz w eksportowanych raportach.
- b) Eksport raportów musi być dostępny co najmniej w następujących formatach:
  - CSV – do analiz danych i integracji z systemami zewnętrznymi,
  - JSON – do integracji z API i wykorzystania programistycznego,
  - PDF – do raportów operacyjnych i prezentacji kierownictwu,
- c) Eksport danych z dashboardów do formatu PDF jest obowiązkowy i musi zachowywać formatowanie, wykresy oraz układ wizualny.
- d) Eksport do formatu DOC(X) jest zalecany. W przypadku braku natywnego wsparcia, system powinien umożliwiać eksport do szablonu (np. \*.docx) lub do uporządkowanego formatu danych, umożliwiającego Zamawiającemu łatwe przekształcenie do dokumentu Word.
- e) System musi umożliwiać planowanie i automatyczne generowanie raportów w zadanych odstępach czasu (np. codziennie, tygodniowo) oraz ich dystrybucję do wskazanych odbiorców (np. e-mail, folder sieciowy).
- f) Eksportowane raporty muszą zawierać pełen kontekst incydentu, w tym:
  - historię działań,
  - wyniki playbooków,
  - przypisane IOC,
  - komentarze analityków,
  - metadane (czas utworzenia, właściciel, status).

#### 2.5. Architektura, niezawodność i monitorowanie

##### 2.5.1. Niezawodność i bezpieczeństwo działania

System SOAR musi zapewniać wysoką dostępność, odporność na awarie i bezpieczeństwo działania, zgodnie z wymogami środowisk SOC oraz standardami, w tym NIS2.

- a) System musi umożliwiać wdrożenie mechanizmów zapewniających wysoką dostępność (HA) lub wspierać architekturę zapewniającą ciągłość działania, np. poprzez redundancję kluczowych komponentów lub integrację z platformą wirtualizacyjną.
- b) System musi obsługiwać mechanizmy backupu i odtwarzania po awarii z wykorzystaniem narzędzi dostępnych w infrastrukturze Zamawiającego — w szczególności z platformą Veeam Backup&Replication. Wykonawca jest zobowiązany do:
  - wdrożenia i konfiguracji integracji z Veeam,
  - zapewnienia regularnych kopii zapasowych wszystkich komponentów systemu (dane, konfiguracja, playbooki, logi),
  - zagwarantowania możliwości pełnego odtworzenia systemu (aplikacja + dane),
- c) System musi wspierać zdalne i lokalne zarządzanie z użyciem m.in.:
  - SSHv2,
  - HTTPS (GUI),
  - SNMP v2/v3,

- zewnętrznych serwerów uwierzytelniania (Active Directory, LDAP, RADIUS),
- synchronizacji czasu z serwerami NTP/SNTP.

d) System powinien umożliwiać integrację z nowoczesnymi metodami uwierzytelniania i autoryzacji, w szczególności w kontekście API, takimi jak

- OAuth2,
- certyfikaty X.509 lub równoważne mechanizmy.

#### 2.5.2. Monitorowanie zasobów i kondycji systemu

System SOAR musi umożliwiać kompleksowe monitorowanie swojego stanu i wydajności:

a) System musi umożliwiać monitorowanie m.in.:

- wykorzystania zasobów systemowych (CPU, RAM, dysk, sieć),
- obciążenia kolejek przetwarzania,
- liczby aktywnych incydentów i uruchomionych playbooków.

b) System musi generować alerty w przypadku:

- przekroczenia progów wydajnościowych (np. CPU > 90%, zużycie dysku > 80%),
- wystąpienia błędów i awarii systemowych (np. błąd integracji, awaria komponentu, brak komunikacji z SIEM).

c) Alerty i logi systemowe muszą być:

- rejestrowane wewnętrznie,
- przesyłane do zewnętrznego systemu monitoringu (np. SIEM – Energy Logserver) za pomocą Syslog, REST API lub równoważnych mechanizmów,
- możliwe do korelacji z innymi zdarzeniami bezpieczeństwa.

d) System musi umożliwiać raportowanie dostępności i kondycji systemu (np. uptime, liczba incydentów technicznych), zgodnie z wymaganiami operacyjnymi Zamawiającego, w tym możliwość eksportu danych do raportów.

#### 2.6. Zarządzanie użytkownikami i uprawnieniami

System SOAR musi umożliwiać szczegółowe zarządzanie dostępem do funkcji i danych systemu w oparciu o przypisane role oraz integrować się z zewnętrznymi mechanizmami uwierzytelniania.

##### 2.6.1. Model RBAC

- a) System musi wspierać model RBAC (Role-Based Access Control), zgodny z zasadą minimalnych uprawnień (principle of least privilege), umożliwiający przypisywanie użytkownikom tylko tych uprawnień, które są niezbędne do wykonywania ich zadań.
- b) Dopuszcza się wdrożenie modelu RBAC przy użyciu zewnętrznych narzędzi (np. Kibana, LDAP), jeśli brak jest gotowego rozwiązania w systemie, o ile zapewnia to równoważny poziom kontroli i audytu.

##### 2.6.2. Zakres kontroli dostępu

System musi umożliwiać modyfikację uprawnień dostępu do co najmniej następujących elementów:

- a) playbooków,
- b) skryptów automatyzacji,
- c) komend w ramach integracji,
- d) elementów interfejsu użytkownika.
- e) repozytoriów CTI i feedów danych,
- f) konfiguracji systemu i parametrów globalnych.

##### 2.6.3. Integracja z systemami zewnętrznymi



- a) System musi umożliwiać powiązanie ról RBAC z jednostkami w systemach zewnętrznych, takich jak:
  - grupy w Active Directory,
  - atrybuty w SAML,
  - profile w LDAP,
  - konta w RADIUS.
- b) W przypadku braku natywnej integracji, dopuszcza się realizację tego wymogu przez autorskie mechanizmy autoryzacji lub komponent pośredniczący (np. proxy), o ile zapewnia to bezpieczne i audytowalne przekazywanie informacji o roli użytkownika.

#### 2.6.4. Audyt i rejestracja zdarzeń

System musi rejestrować pełną aktywność użytkowników, w szczególności:

- a) logowanie i wylogowanie,
- b) tworzenie, edycję i usuwanie obiektów systemowych (np. playbooki, skrypty, integracje),
- c) instalację nowych integracji,
- d) zmiany w konfiguracji systemu.
- e) zmiany uprawnień użytkowników i ról (przywilejów),
- f) próby nieautoryzowanego dostępu do funkcji, danych lub zasobów systemu,
- g) próby eksportu danych lub logów.

#### 2.7. Bezpieczeństwo łańcucha dostaw i zarządzanie dostawcami

2.7.1. Wykonawca zobowiązuje się do zapewnienia bezpieczeństwa, zgodnie z wymogami Dyrektywy (UE) 2022/2555 (NIS2).

2.7.2. Wykonawca przedstawi Zamawiającemu listę bezpośrednich dostawców komponentów sprzętowych i programowych wykorzystywanych w realizowanych zadaniach, wraz z:

- a) nazwą dostawcy,
- b) zakresem dostarczanych komponentów lub usług,
- c) wersjami oprogramowania i datami wsparcia technicznego,
- d) informacjami o stosowanych licencjach (w tym komponenty Open Source).

2.7.3. W przypadku wykrycia podatności lub naruszenia bezpieczeństwa przez podwykonawcę, Wykonawca zobowiązuje się do niezwłocznego powiadomienia Zamawiającego.

2.7.4. Wykonawca stosuje zasady Zero Trust.

2.7.5. Wykonawca zapewnia, że wszystkie komponenty sprzętowe i programowe spełniają aktualne wymagania bezpieczeństwa.

#### 2.8. Uczenie maszynowe (ML)

System SOAR powinien wykorzystywać mechanizmy uczenia maszynowego (Machine Learning) w celu zwiększenia efektywności operacji SOC, skrócenia czasu reakcji (MTTR) oraz wsparcia analityków poprzez automatyczne sugestie i rekomendacje.

ML nie może pełnić roli decyzyjnej – wszystkie rekomendacje muszą być weryfikowane i potwierdzane przez operatora SOC.

##### 2.8.1. Wsparcie analityków SOC

System powinien wykorzystywać algorytmy ML do wspierania analityków, w szczególności poprzez:

- a) sugerowanie komend podczas analizy incydentów na podstawie danych historycznych (np. najczęściej wykonywane akcje dla danego typu incydentu),
- b) proponowanie działań w oparciu o wytrenowane modele lub wzorce behawioralne (np. typowe sekwencje ataku, anomalie w zachowaniu użytkowników),

- c) automatyczne przypisywanie priorytetów incyidentom na podstawie typu zagrożenia, źródła alertu i historii reakcji.
- d) identyfikację powiązanych incyidentów i korelację zdarzeń na podstawie wspólnych cech (np. ten sam adres IP, użytkownik, host).

#### 2.8.2. Zakres zastosowania ML

Dopuszcza się wykorzystanie uczenia maszynowego do generowania podpowiedzi dotyczących m.in.:

- a) wskaźników kompromitacji (IOC) – np. sugerowanie nowych IOC na podstawie podobieństwa do znanych wzorców,
- b) kampanii i incyidentów – grupowanie incyidentów w kampanie na podstawie wspólnych TTP (Tactics, Techniques, Procedures),
- c) alarmów i podatności – identyfikacja fałszywych alarmów (false positives) lub korelacja alertów z danymi o podatnościach (np. z Nessusa),
- d) zasobów (assetów) – ocena krytyczności hosta na podstawie jego roli, danych i historii incyidentów,
- e) zadań przypisanych w ramach procesu obsługi incydentu – sugerowanie właściciela incydentu lub zespołu do eskalacji.

#### 2.8.3. Kontrola i bezpieczeństwo decyzji ML

- a) System musi umożliwiać ręczne nadpisanie każdej rekomendacji ML przez analityka SOC.
- b) Wszystkie sugestie ML muszą być oznaczone jako „pomocnicze” i nie mogą prowadzić do automatycznego wykonywania działań naprawczych bez potwierdzenia.
- c) System musi zapewniać przezroczystość działania modeli ML, w tym możliwość wyświetlenia podstawy decyzji (np. „sugerowane działanie wynika z 80% podobieństwa do wcześniejszych incyidentów”).
- d) Modele ML muszą być aktualizowane przez producenta lub możliwe do ponownego trenowania przez administratora systemu.

### 2.9. Dodatkowe funkcjonalności operacyjne

#### 2.9.1. Tworzenie kopii zapasowych

System musi umożliwiać tworzenie automatycznych i cyklicznych kopii zapasowych danych i konfiguracji, umożliwiających szybkie odzyskanie systemu po awarii.

#### 2.9.2. Obsługa komponentu PROXY

System musi wspierać komponent typu PROXY, pośredniczący w komunikacji między serwerem SOAR a zewnętrznymi systemami działającymi w odseparowanych segmentach sieci (np. systemy w DMZ, sieci zarządzania).

- a) Funkcjonalność PROXY może być realizowana poprzez dedykowany komponent (np. reverse proxy) lub mechanizmy REST API.
- b) PROXY musi obsługiwać szyfrowanie komunikacji (TLS 1.2+) i wspierać bezpieczne mechanizmy uwierzytelniania (np. certyfikaty X.509, API keys).
- c) Komunikacja przez PROXY musi być monitorowana i rejestrowana, a wszystkie zdarzenia muszą być przesyłane do systemu SIEM (Energy Logserver).
- d) PROXY musi być częścią całościowej architektury bezpieczeństwa i podlegać regularnym audytom.

### 3. WYMAGANIA TECHNICZNE SPRZĘT

#### 3.1. Wymagania sprzętowe

Wykonawca zobowiązany jest do dostarczenia dedykowanego sprzętu serwerowego przeznaczonego do wdrożenia systemu SOAR.

Nie dopuszcza się wdrożenia rozwiązania wyłącznie w formie oprogramowania – fizyczne urządzenie musi być dostarczone.

Dostarczony sprzęt musi:

##### 3.1.1. Spełniać wymagania producenta systemu SOAR, uwzględniając rzeczywiste potrzeby Zamawiającego, w tym:

- a) obsługę wolumenu danych wynikającego ze statystyk działania obecnego środowiska SOC, w szczególności:
  - średnio 35 000 alertów dziennie,
  - co najmniej 1 000 000 alertów miesięcznie,
  - szacunkowo 12,5 mln alertów rocznie,
- b) zapewnienie przestrzeni dyskowej umożliwiającej przechowywanie danych:
  - min. 100 dni przechowywania danych monitorowanych online (incydenty, playbooki, akcje, historie, metadane, artefakty, materiał dowodowy),
  - min. 730 dni przechowywania danych historycznych (zamknięte incydenty, przebieg reakcji, analizy, raporty). liczby obsługiwanych incydentów i alertów,
- c) zapewnienie wydajności systemu umożliwiającej:
  - obsługę średniego wolumenu danych na poziomie 5000 zdarzeń na sekundę (EPS),
  - obsługę szczytowego obciążenia do 10 000 EPS, bez konieczności rozbudowy sprzętowej, gwarantując stabilność działania i niski czas reakcji w warunkach maksymalnego obciążenia.

Wskazane wartości stanowią odniesienie do całkowitej liczby zdarzeń przetwarzanych w środowisku SIEM, z którego system SOAR otrzymuje alerty i dane kontekstowe. Wymagania te mają na celu zapewnienie sprawnego działania systemu SOAR, w tym szybkiego przetwarzania incydentów, równoległej obsługi wielu playbooków oraz efektywnej komunikacji z systemami zewnętrznymi.

##### 3.1.2. Wymagane minimalne parametry techniczne dla zaoferowanych serwerów:

- a) Procesor: min. 1× Intel Xeon Silver 4316 lub AMD EPYC o równoważnej wydajności ( $\geq 20$  rdzeni,  $\geq 2.3$  GHz, cache L3  $\geq 30$  MB).
- b) Pamięć RAM: min. 32 GB DDR4/DDR5 z ECC, taktowanie  $\geq 3200$  MT/s, możliwość rozbudowy do  $\geq 128$  GB.
- c) Dyski: min. 8 zatok hot-swap 2.5" SAS/SATA/SSD; minimalna konfiguracja:
  - 2× SSD 960 GB SATA (read intensive)
  - 2× HDD 600 GB SAS 10k RPM
  - możliwość rozbudowy
- d) RAID: sprzętowy kontroler RAID z min. 8 GB cache, obsługa RAID 1, 5, 6, 10 lub wyższych, BBU opcjonalnie.
- e) Zasilanie i sieć:
  - 2× redundantne zasilacze hot-swap 700 W, certyfikat 80 PLUS Titanium
  - min. 2× port RJ-45 1 GbE, opcjonalnie 2× port SFP+ 10 GbE
- f) Karta sieciowa: obsługa Wake-on-LAN, PXE boot, TCP/IP offloading.
- g) Zarządzanie zdalne:

- zintegrowana karta zarządzająca (iDRAC9 Enterprise lub iRMC Advanced Pack)
- dedykowany port RJ-45 do zarządzania
- obsługa trybu bezagentowego
- wsparcie dla narzędzi do monitorowania i zarządzania.
- obudowa: rack 19", wysokość 1U lub 2U, zestaw szyn montażowych w komplecie.

### 3.1.3. Wymagania sieciowe

System musi zapewniać wsparcie dla:

- VLAN (IEEE 802.1Q) – do segmentacji ruchu,
- agregacji linków (LACP, IEEE 802.3ad) – dla zwiększenia przepustowości i niezawodności,
- Quality of Service (QoS) – do priorytetyzacji ruchu krytycznego (np. integracje, zarządzanie),
- protokołu IPv6 – zarówno w komunikacji, jak i konfiguracji.

### 3.1.4. Kompatybilność z infrastrukturą Zamawiającego

Wykonawca zobowiązany jest do zapewnienia pełnej kompatybilności dostarczonych urządzeń z istniejącą u Zamawiającego konsolą KVM ATEN CL1008 wyposażoną w porty SPHD-17, wykorzystywaną w infrastrukturze serwerów SIEM.

Wykonawca musi dostarczyć wszystkie niezbędne kable i/lub adaptery umożliwiające prawidłowe podłączenie dostarczonych komponentów do wskazanej konsoli.

## 4. LICENCJE

### 4.1. Licencje dla użytkowników i wsparcie producenta

Wykonawca zobowiązany jest do dostarczenia licencji dla 6 operatorów SOC, w tym co najmniej 2 administratorów, wraz z trzyletnim wsparciem producenta, liczonym od dnia odbioru Zadania III.

Licencje muszą obejmować pełną funkcjonalność systemu, w tym wszystkie moduły związane z automatyzacją, integracją, raportowaniem, threat intelligence i analizą incydentów.

### 4.2. Akceptowane modele licencjonowania

Zamawiający akceptuje następujące modele licencjonowania:

- a) licencję wieczystą (perpetual license) – niewprowadzającą żadnych ograniczeń ilościowych ani funkcjonalnych, w szczególności dotyczących liczby incydentów, zdarzeń danych czy liczby integracji,
- b) model subskrypcyjny, pod warunkiem że nie wprowadza on jakichkolwiek ograniczeń funkcjonalnych ani ilościowych, w szczególności w odniesieniu do:
  - liczby incydentów,
  - liczby playbooków, skryptów i scenariuszy automatyzacji,
  - liczby integracji z narzędziami bezpieczeństwa,
  - ilości przetwarzanych danych w ramach tych integracji,
  - liczby podłączonych konektorów,
  - liczby maszyn wykorzystywanych w architekturze systemu,
  - rozmiaru przestrzeni dyskowej.

Licencje muszą być wolne od ograniczeń terytorialnych i obowiązywać przez okres nie krótszy niż 36 miesięcy, liczony od dnia podpisania przez Zamawiającego protokołu odbioru Zadania III (tj. od daty ich aktywacji). Dopuszcza się także licencje bezterminowe oraz o dłuższym okresie obowiązywania.

### 4.3. Aktywacja licencji

- a) Wykonawca zobowiązuje się do aktywacji licencji w ciągu 5 dni roboczych od daty podpisania protokołu odbioru Zadania III.
- b) W przypadku opóźnienia aktywacji, Wykonawca ponosi pełną odpowiedzialność za wszelkie konsekwencje techniczne i operacyjne.
- c) Wykonawca zobowiązuje się do dostarczenia wszystkich niezbędnych kluczy aktywacyjnych, licencji i dokumentów licencyjnych przed aktywacją systemu.
- d) Wszystkie nośniki z licencjami, instalatorami i sterownikami (CD/DVD, pendrive) stają się własnością Zamawiającego.

### 4.4. Brak ograniczeń licencyjnych

Oferowany System SOAR nie może zawierać żadnych ograniczeń licencyjnych, w szczególności w zakresie:

- a) liczby:
  - incydentów,
  - scenariuszy (playbooków), skryptów i akcji automatyzacji,
  - integracji z narzędziami bezpieczeństwa,
  - konektorów,
- b) ilości danych przetwarzanych w ramach integracji,
- c) rozmiaru przestrzeni dyskowej,
- d) System SOAR nie może zawierać ograniczeń licencyjnych na dodawanie komponentów przetwarzania (processing nodes) lub równoważnych mechanizmów, o ile są one wspierane przez daną wersję oprogramowania.

#### 4.5. Gwarancja ciągłości wsparcia i rozwoju

- a) Na dzień składania oferty system SOAR nie może być przez producenta oznaczony jako „End of Life” (EOL) ani „End of Support” (EOS). Ponadto żadna data zakończenia rozwoju lub wsparcia technicznego tej wersji nie może być publicznie ogłoszona przez producenta.
- b) Wykonawca zobowiązuje się, że przez cały okres obowiązywania umowy (36 miesięcy):
  - dostarczony system SOAR będzie objęty pełnym wsparciem technicznym producenta,
  - Zamawiający będzie miał dostęp do:
    - nowych wersji oprogramowania,
    - poprawek bezpieczeństwa,
    - aktualizacji funkcjonalnych,
    - dokumentacji technicznej oraz bazy wiedzy producenta.
- c) Wykonawca gwarantuje, że krytyczne poprawki bezpieczeństwa oraz istotne aktualizacje funkcjonalne będą udostępniane dla wszystkich wspieranych wersji systemu (w tym on-premise) równocześnie lub w nieznacznym odstępie czasowym (nie później niż 90 dni) od ich udostępnienia w innych wariantach (np. SaaS), chyba że producent jednoznacznie uzasadni dłuższy termin, wskazując obiektywne ograniczenia architektoniczne.
- d) W przypadku ogłoszenia przez producenta decyzji o zaprzestaniu rozwoju lub wsparcia technicznego którejkolwiek z wersji systemu SOAR w trakcie obowiązywania umowy, Wykonawca zobowiązuje się niezwłocznie poinformować Zamawiającego (nie później niż 7 dni roboczych od daty ogłoszenia).



## 5. HARMONOGRAM REALIZACJI ZADAŃ

Poniższy harmonogram określa maksymalne terminy realizacji poszczególnych zadań w ramach przedmiotu zamówienia. Terminy liczone są od dnia zawarcia umowy.

Nr zadania	Nazwa zadania	Termin realizacji	Opis
I	Opracowanie projektu technicznego Systemu SOAR	do 6 tygodni od dnia zawarcia umowy	Architektura rozwiązania, integracje, konfiguracja środowiska. Wymaga formalnego odbioru przez Zamawiającego – warunek przejścia do dalszych zadań.
II	Dostawa Systemu SOAR	do 6 tygodni od dnia zawarcia umowy	Oprogramowanie z licencjami, sprzęt, trzyletnie wsparcie producenta (rozliczane rocznie). Wymaga formalnego odbioru.
III	Wdrożenie Systemu SOAR	do 10 tygodni od dnia odbioru Zadania II	Instalacja i wstępna konfiguracja Systemu zgodnie z projektem technicznym. Wymaga formalnego odbioru.
IV	Integracja z systemami bezpieczeństwa	w ramach Zadania III	Zadanie IV stanowi podzadanie w ramach Zadania III. Połączenie z SIEM, EDR, WAF, firewall, systemami zgłoszeniowymi itd. Wymaga formalnego odbioru.
V	Optymalizacja działania Systemu SOAR	do 4 tygodni od zakończenia Zadania III	Zaawansowana parametryzacja, testy, dobre praktyki, rekomendacje rozwoju. Wymaga formalnego odbioru.
VI	Opracowanie dokumentacji powykonawczej	do 4 tygodni od zakończenia Zadania V – nie dłużej niż 20 tygodni od dnia zawarcia umowy	Kompletny opis konfiguracji, integracji, działania, procedur eksploatacyjnych. Może być realizowane równolegle z Zadaniem VII.
VII	Przeprowadzenie instruktażu	do dnia odbioru Zadania VI – nie dłużej niż 22 tygodni od dnia zawarcia umowy	Szkolenie/warsztaty z obsługi i administracji dla min. 8 operatorów i administratorów SOC. Wymaga formalnego odbioru. Może być realizowane równolegle z Zadaniem VI.
VIII	Gwarancja i asysta techniczna	przez 36 miesięcy od dnia odbioru zadania V	Gwarancja na cały system (sprzęt i oprogramowanie), wsparcie producenta systemu (aktualizacje, poprawki, konsultacje) oraz asysta techniczna Wykonawcy zgodnie z rozdziałem 13.

Potwierdzeniem wykonania wszystkich Zadań określonych w Opisie przedmiotu zamówienia będzie, podpisany z wynikiem pozytywnym przez przedstawicieli Zamawiającego i Wykonawcy Końcowy protokół odbioru.

## 6. ZADANIE I - OPRACOWANIE PROJEKTU TECHNICZNEGO SYSTEMU SOAR

W ramach Zadania I Wykonawca opracuje i przekaze Zamawiającemu Projekt Techniczny Systemu SOAR, zawierający dokumentację analityczną i techniczną, przygotowaną zgodnie z wymaganiami niniejszego Opisu Przedmiotu Zamówienia (OPZ), a także na podstawie analizy środowiska teleinformatycznego Zamawiającego, przeprowadzonej wspólnie przez strony zgodnie z pkt 6.2.1.

Projekt Techniczny będzie stanowić podstawę do realizacji kolejnych zadań, w tym dostawy (Zadanie II), wdrożenia (Zadanie III), integracji (Zadanie IV) oraz optymalizacji (Zadanie V) Systemu SOAR.

### 6.1. Wymagania ogólne

- a) Projekt nie może wprowadzać zmian skutkujących utratą gwarancji, sprawności lub poprawności działania istniejących systemów Zamawiającego.
- b) Wszystkie założenia projektowe muszą być zgodne z wymaganiami pozostałych zadań określonych w OPZ (w szczególności z Zadaniami II–V) oraz uprzednio uzgodnione z Zamawiającym.
- c) Spotkania robocze będą prowadzone stacjonarnie w siedzibie GUS lub zdalnie – według decyzji Zamawiającego.
- d) Projekt Techniczny musi obejmować co najmniej:
  - architekturę systemu,
  - plan integracji,
  - harmonogram wdrożenia i testów.

### 6.2. Zakres prac projektowych

6.2.1. Wykonawca przeprowadzi szczegółową analizę środowiska Zamawiającego, obejmującą:

- a) identyfikację źródeł logów i metadanych z systemów i urządzeń przekazywanych do Systemu SOAR,
- b) ocenę możliwości automatyzacji działań (np. dostępność API, webhooków, skryptów, SSH, SNMP),
- c) przegląd dostępnych interfejsów integracyjnych (REST API, SOAP, syslog, JSON),
- d) ocenę skalowalności rozwiązania (liczba incydentów, wolumen danych, liczba integracji),
- e) charakterystykę parametrów komunikacyjnych (adresy IP, porty, protokoły, polityki dostępu),
- f) wymagania bezpieczeństwa (uwierzytelnianie, autoryzacja, szyfrowanie transmisji, segmentacja sieci).

Zamawiający zapewni niezbędne dane wejściowe, w tym informacje dotyczące:

- infrastruktury serwerowej i logującej,
- konfiguracji systemu SIEM (Elastic),
- posiadanych systemów bezpieczeństwa (WAF, EDR, firewall, VPN, DLP, AV).

Wykonawca potwierdzi, że SIEM (Energy Logserver) będzie głównym źródłem danych dla Systemu SOAR. Integracja z innymi systemami bezpieczeństwa (np. EDR, WAF, FW, DLP) będzie realizowana w pierwszej kolejności poprzez SIEM, chyba że bezpośrednie połączenie jest niezbędne do prawidłowego działania playbooka.

Lista źródeł logów i systemów przeznaczonych do integracji musi zostać zatwierdzona przez Zamawiającego. Wykonawca przekaze protokół z przeprowadzonej analizy środowiska, zawierający w szczególności:

- wykaz systemów i źródeł logów,
- możliwe scenariusze integracji,
- ograniczenia techniczne i rekomendacje,
- wnioski dotyczące wydajności i skalowalności.

### 6.2.2. Treść Projektu technicznego

Projekt techniczny powinien zawierać:

- a) Koncepcję architektury wdrożenia, z podziałem na warstwy logiczne (zbieranie danych, korelacja, automatyzacja, prezentacja, zarządzanie);
- b) Schematy połączeń sieciowych i integracji (adresacja, porty, typy transmisji, szyfrowanie);
- c) Wykaz komponentów sprzętowych i programowych (CPU, RAM, dyski, interfejsy, typ wirtualizacji, licencje), (zgodnie z wymaganiami Zadania II);
- d) Listę integrowanych systemów wraz z zakresem wymiany danych, protokołami i metodami uwierzytelniania (np. API key, tokeny, certyfikaty, konta serwisowe); Lista integrowanych systemów powinna obejmować nie tylko SIEM, ale również inne kluczowe systemy bezpieczeństwa o ile jest to wymagane dla realizacji przypadków użycia i automatyzacji.
- e) Plan podłączenia do infrastruktury LAN Zamawiającego (VLAN-y, redundancja, segmentacja, lokalizacja logiczna);
- f) Opis konfiguracji komponentów Systemu SOAR (silniki reguł, orchestrator, integratory, kolejki danych, bufor, klasy przechowywania);
- g) Politykę retencji danych (dane surowe, przetworzone, metadane, artefakty incydentów; czasy przechowywania i mechanizmy usuwania);
- h) Opis mechanizmów backupu i odzyskiwania danych (lokalizacja, harmonogram, sposób odtwarzania);
- i) Zasady bezpieczeństwa systemu (LDAP/AD, RBAC, MFA, szyfrowanie danych, logowanie, audyt);
- j) Plan rozmieszczenia sprzętu w szafach RACK (zasilanie, chłodzenie, dostęp fizyczny, nośność);
- k) Harmonogram wdrożenia z podziałem na etapy (instalacja, konfiguracja, testy funkcjonalne i integracyjne, uruchomienie produkcyjne (rollout etapowy)).

Projekt techniczny musi spełniać minimalne wymagania szczegółowości, w tym zawierać:

- diagramy i schematy architektury systemu oraz połączeń sieciowych,
- przykładowe wzory konfiguracji dla kluczowych komponentów (np. integratorów, reguł korelacyjnych, playbooków),
- opisy przepływów danych i integracji w formie graficznej i tabelarycznej,
- format dokumentu edytowalny, preferowany docx. Schematy, diagramy, modele, paczki wymagań w podziale na wymagania funkcjonalne i нефункционалне zostaną dodatkowo utworzone w EA. Każde wymaganie będzie opisane w następujący sposób: nazwa wymagania w EA to nr wymagania z projektu technicznego, treść wymagania zostanie dodane w polu niżej. Wymaganie w EA zostanie uzupełnione o atrybuty typ i priorytet zgodnie z projektem technicznym

### 6.2.3. Plan testów funkcjonalnych

Testy funkcjonalne, integracyjne, automatyzacyjne i wydajnościowe powinny być przeprowadzane nie tylko w ramach odbioru wdrożenia, ale również po każdej istotnej zmianie w konfiguracji systemu (np. dodanie nowej integracji, wdrożenie nowego playbooka, zmiana wersji systemu). Celem testów jest w szczególności wykrycie wąskich gardeł wydajnościowych, błędów konfiguracyjnych oraz zdarzeń fałszywie pozytywnych/negatywnych.

Projekt musi zawierać szczegółowy plan testów, obejmujący:

- a) Testy funkcjonalne komponentów
  - Weryfikacja działania podstawowych komponentów: korelatora, orkiestratora, bazy danych, interfejsu GUI;
  - Sprawdzenie funkcji zarządzania incydentami: eskalacja, przypisanie, zmiana statusu, zamykanie;
  - Ocena działania funkcji raportowania i dashboardów (np. czas obsługi, liczba incydentów per źródło, zgodność z SLA).
- b) Testy integracyjne

- Poprawność integracji z systemem Elastic SIEM (odbiór, klasyfikacja, przekazanie zdarzeń);
- Weryfikacja przepływu danych z EDR, firewalli, WAF i systemów ticketowych;
- Sprawdzenie działania mechanizmów autoryzacji (OAuth2, certyfikaty X.509);
- Wykorzystanie danych Threat Intelligence (IOC/IOA) w detekcji i automatyzacji.

c) Testy automatyzacji

- Skuteczność działania automatyzacji (uruchamianie playbooków, powiadamianie zespołów).
- Weryfikacja działania playbooków w trybie debug;
- Testowanie reakcji na fałszywe alerty (false positives).

d) Testy odporności i bezpieczeństwa

- Testy HA, failover, backup i przywracanie systemu;
- Weryfikacja procedur i mechanizmów backupu i odtwarzania Systemu SOAR z kopii zapasowej.

e) Testy wydajnościowe

- Symulacja obciążenia systemu (np. generowanie zdarzeń),
- Weryfikacja liczby przetworzonych zdarzeń w czasie rzeczywistym oraz czasów reakcji systemu,
- Identyfikacja wąskich gardeł (np. kolejki przetwarzania, opóźnienia integracji).

### 6.3. Odbiór Projektu technicznego

- a) Projekt należy przekazać w terminie do 2 tygodni od podpisania umowy.
- b) Zamawiający zgłasza uwagi w ciągu 2 dni roboczych.
- c) Wykonawca wprowadza poprawki w ciągu kolejnych 3 dni roboczych.
- d) Przewidziano maksymalnie dwie iteracje korekt.
- e) Brak akceptacji po poprawkach skutkuje przekazaniem Projektu do ponownej korekty (czas: 2 dni robocze).
- f) Dokumentacja musi być dostarczona w formacie edytowalnym i PDF, na nośniku USB.
- g) Odbiór zostaje potwierdzony protokołem odbioru Zadania I.

## 7. ZADANIE II - DOSTAWA SYSTEMU SOAR

W ramach Zadania II Wykonawca dostarczy kompletne środowisko sprzętowo-programowe Systemu SOAR (Security Orchestration, Automation and Response), zgodnie z Projektem Technicznym.

### 7.1. Wymagania ogólne dotyczące dostawy:

- 7.1.1. Dostawa obejmuje wszystkie niezbędne komponenty sprzętowe oraz oprogramowanie wraz wymaganymi licencjami
- 7.1.2. Wszystkie dostarczone elementy muszą w pełni kompatybilne ze sobą oraz zgodne w wymaganiami określonymi w Projekcie Technicznym.
- 7.1.3. Dostarczony sprzęt musi być fabrycznie nowy (wyprodukowany nie wcześniej niż 12 miesięcy przed dostawą), oryginalnie zapakowany, pochodzić z autoryzowanego kanału sprzedaży na rynek polski lub unijny i spełniać wymagania przepisów obowiązujących w UE.
- 7.1.4. Wraz z oprogramowaniem należy dostarczyć wszystkie niezbędne nośniki (np. CD/DVD, pendrive) zawierające licencje, instalatory oraz sterowniki. Wszystkie te elementy przechodzą na własność Zamawiającego.
- 7.1.5. Licencje muszą umożliwiać korzystanie z pełnej funkcjonalności systemu przez okres co najmniej 36 miesięcy.
- 7.1.6. Sprzęt musi być zgodny z siecią zasilającą 230 V  $\pm 10\%$ , 50 Hz.

### 7.2. Wymagania dotyczące dostawy sprzętu i oprogramowania

- 7.2.1. Wszystkie dostarczone komponenty sprzętowe muszą zawierać niezbędne akcesoria (np. kable zasilające, interfejsowe, mocowania rack, zestawy montażowe).
- 7.2.2. Wykonawca zapewni kompletne okablowanie sieciowe (patchcords, peszle itp.).
- 7.2.3. System zostanie podłączony do infrastruktury Zamawiającego za pośrednictwem interfejsów RJ45 lub SFP/SFP+ (1 Gbps / 10 Gbps).
- 7.2.4. Dostarczone urządzenia muszą być gotowe do instalacji w szafach rack w lokalizacji Zamawiającego.
- 7.2.5. Sprzęt zostanie dostarczony w dni robocze w godzinach 08:15–16:00, do siedziby Zamawiającego.
- 7.2.6. Wykonawca zapewni transport, rozładunek oraz wniesienie sprzętu na 1. piętro budynku Głównego Urzędu Statystycznego.
- 7.2.7. Rozpakowanie i uruchomienie sprzętu wykona wyłącznie Wykonawca.

### 7.3. Dokumentacja i odbiór dostawy

#### 7.3.1. Wraz z dostawą Wykonawca przekaże:

- a) wykaz dostarczonych komponentów (z numerami seryjnymi),
- b) dokumenty potwierdzające legalność oprogramowania
- c) instrukcje producenta w wersji elektronicznej
- d) karty gwarancyjne dla dostarczonych urządzeń i/lub komponentów.

#### 7.3.2. Dostawa zostanie potwierdzona przez obie Strony podpisaniem Protokołu odbioru dostawy - zadania II

## 8. ZADANIE III - WDROŻENIE SYSTEMU SOAR

W ramach Zadania III Wykonawca przeprowadzi instalację i konfigurację Systemu SOAR zgodnie z Projektem Technicznym, obejmującą uruchomienie środowiska. Zadanie obejmuje również wstępne testy funkcjonalne i stanowi podstawę do realizacji integracji (Zadanie IV), które są jego integralną częścią.

### 8.1. Zakres zadania

- a) Instalacja Systemu SOAR na dostarczonym sprzęcie.
- b) Konfiguracja komponentów Systemu zgodnie z Projektem Technicznym, w tym m.in. repozytoriów danych, interfejsów komunikacyjnych, kont użytkowników, polityk dostępu.
- c) Wstępna parametryzacja systemu obejmująca konfigurację podstawowych reguł, źródeł danych, harmonogramów oraz interfejsów użytkownika.
- d) Uruchomienie Systemu SOAR w trybie operacyjnym w środowisku Zamawiającego, zgodnie z poniższym harmonogramem:
  - Instalacja i konfiguracja – przygotowanie środowiska, instalacja komponentów, integracja z SIEM (Energy Logserver) jako głównym źródłem danych,
  - Pilotaż – testowe uruchomienie dla ograniczonej grupy operatorów SOC, przeprowadzenie testów funkcjonalnych, bezpieczeństwa i wydajności, oraz testów akceptacji użytkownika końcowego, zebranie feedbacku oraz wprowadzenie poprawek,
  - Rollout (stopniowe wdrożenie)
    - stopniowe uruchomienie dostępu dla kolejnych użytkowników,
    - aktywacja i testy integracji z systemami bezpieczeństwa (EDR, firewall, WAF itd.),
    - optymalizacja konfiguracji na podstawie doświadczeń z pilotażu,
    - przygotowanie systemu do pełnej eksploatacji, w tym zakończenie wszystkich integracji wymaganych w Zadaniu IV.

W ramach etapu rollout, zgodnie z Zadaniem IV, zostaną aktywowane i przetestowane wszystkie integracje z systemami bezpieczeństwa.

- Zakończenie wdrożenia – formalny odbiór Zadania III i IV po pozytywnym zakończeniu etapu rollout i integracji.

### 8.2. Wymagania szczegółowe

- a) Wszystkie działania muszą być realizowane z zachowaniem ciągłości działania istniejących systemów Zamawiającego.
- b) Wykonawca zapewni poprawność działania wdrożonego Systemu oraz gotowość do jego dalszego rozwoju w ramach kolejnych zadań.
- c) Wszelkie instalacje i konfiguracje muszą być udokumentowane i przekazane Zamawiającemu w formie instrukcji administracyjnych.
- d) Wykonawca przeprowadzi kompleksowe testy poprawności działania systemu, obejmujące:
  - funkcjonalność podstawowych komponentów (GUI, baza danych, orchestrator),
  - działanie mechanizmów zarządzania incydentami,
  - przepływ danych z SIEM,
  - poprawność konfiguracji użytkowników i uprawnień,
  - działanie mechanizmów backupu i monitorowania.

### 8.3. Dokumentacja powdrożeniowa

Wykonawca przekaze Zamawiającemu dokumentację powdrożeniową, w tym:

- a) opis środowiska wdrożeniowego (komponenty, adresacja, użytkownicy, zależności),
- b) konfigurację początkową systemu i jego parametryzację,
- c) instrukcję administracyjną i eksploatacyjną (w języku polskim),

### 8.4. Odbiór Zadań III i IV



- a) Odbiór Zadania III (Wdrożenie) i Zadania IV (Integracja) odbywa się łącznie, po zakończeniu wszystkich etapów wdrożenia i potwierdzeniu poprawności działania wszystkich integracji.
- b) Przed podpisaniem Protokołu odbioru Wykonawca przedstawia:
- raport z przeprowadzonych testów funkcjonalnych i integracyjnych,
  - protokoły testów akceptacji użytkownika końcowego (UAT),
  - listę zrealizowanych integracji z potwierdzeniem ich poprawnego działania,
  - dokumentację powdrożeniową.
- c) Podpisanie Protokołu odbioru Zadania III jest możliwe wyłącznie po:
- pełnym uruchomieniu i przetestowaniu wszystkich integracji wymienionych w Zadaniu IV,
  - potwierdzeniu, że system działa zgodnie z Projektem Technicznym i wymaganiami OPZ.

## 9. ZADANIE IV – INTEGRACJA SYSTEMU SOAR Z POSIADANYMI SYSTEMAMI BEZPIECZEŃSTWA - REALIZACJA I WERYFIKACJA INTEGRACJI SYSTEMU SOAR Z SYSTEMAMI BEZPIECZEŃSTWA

W ramach Zadania IV Wykonawca zrealizuje, przetestuje i zweryfikuje integrację wdrożonego Systemu SOAR z posiadanymi przez Zamawiającego systemami bezpieczeństwa, w celu zapewnienia automatyzacji i koordynacji działań związanych z obsługą incydentów.

Zadanie IV realizowane i rozliczane będzie łącznie z zadaniem III – Wdrożeniem Systemu SOAR.

### 9.1. Zakres integracji

Integracja obejmie co najmniej następujące kategorie systemów:

- a) system SIEM – integracja dwukierunkowa (zdarzenia, incydenty, statusy),
- b) systemy ochrony stacji roboczych i serwerów (AV/EDR),
- c) firewall brzegowy klasy NGFW,
- d) Web Application Firewall,
- e) system do skanowania podatności,
- f) system zarządzania zgłoszeniami i incydentami

W przypadku braku stabilnego API lub gotowego konektora, Wykonawca zobowiązany jest do realizacji integracji poprzez mechanizmy BYOI (Bring Your Own Integration), w tym skrypty (Python, PowerShell) lub dedykowane rozwiązania, z zachowaniem bezpieczeństwa i wydajności.

### 9.2. Wymagania integracyjne

- a) Integracje powinny być realizowane przy użyciu dostępnych interfejsów:
  - API (REST, SOAP),
  - konektorów natywnych (jeśli dostępne),
  - webhooków,
  - rozwiązań dedykowanych (np. skrypty, proxy).
- b) System SOAR musi obsługiwać przepływ informacji w czasie quasi-rzeczywistym oraz umożliwiać automatyzację reakcji, np.:
  - blokowanie adresów IP na firewallu,
  - izolowanie hosta za pomocą EDR,
  - aktualizacja statusu incydentu w systemie zgłoszeniowym.
- c) Wykonawca przeprowadzi testy poprawności działania każdej integracji i udokumentuje ich wyniki.
- d) Dla każdej integracji Wykonawca opracuje instrukcję techniczną, zawierającą:
  - sposób działania i zakres funkcjonalny,
  - wymagania techniczne (IP, porty, protokoły, firewall),
  - metody uwierzytelniania (tokeny, certyfikaty, konta serwisowe),
  - schemat przepływu danych,
  - sposób obsługi błędów i monitorowania.
- e) Aby zapobiec nadmiernemu obciążeniu systemów zewnętrznych (np. systemu zgłoszeniowego), automatyczne uruchamianie akcji wyjściowych (np. tworzenie incydentu, blokada IP) wymaga spełnienia co najmniej dwóch z poniższych warunków:
  - priorytet incydentu  $\geq$  P2,
  - co najmniej 3 powiązane alerty w ciągu 15 minut,
  - typ zagrożenia: krytyczny (np. malware, C2, ransomware),
  - brak skutecznej reakcji automatycznej,
  - ręczna eskalacja przez analityka.

- f) Każdy scenariusz integracyjny musi mieć zdefiniowany cel, oczekiwany rezultat, maksymalny czas wykonania oraz mechanizmy obsługi błędów. Reguły muszą zostać udokumentowane w Projekcie Technicznym i zatwierdzone przez Zamawiającego.

#### 9.3. Kryteria akceptacji testów („zaliczony/niezaliczony”)

Aby integracja została uznana za zaliczoną, muszą zostać spełnione następujące mierzalne kryteria:

- Dostępność i stabilność - Integracja działa bez przestojów przez min. 72 godziny testowe
- Czas odpowiedzi - Opóźnienie przekazywania danych  $\leq 60$  sekund
- Kompletność danych -  $\geq 98\%$  danych przekazywanych bez utraty lub uszkodzenia
- Automatyzacja działań - Przynajmniej 2 scenariusze automatyzacji działają poprawnie (np. blokada IP, izolacja hosta)
- Obsługa błędów - Mechanizmy alertowania i reakcji na błędy są zaimplementowane
- Dokumentacja - Instrukcja techniczna i raport testowy są kompletne i zatwierdzone

#### 9.4. Dokumentacja integracyjna

Wykonawca przekazuje Zamawiającemu dokumentację integracji obejmującą co najmniej:

- a) listę zrealizowanych połączeń z systemami źródłowymi,
- b) zastosowane mechanizmy komunikacji i protokoły,
- c) parametry konfiguracyjne konektorów,
- d) schematy danych oraz sposób ich mapowania,
- e) scenariusze testowe wraz z wynikami testów poprawności.
- f) protokół z testów funkcjonalnych, zawierający
  - Opis środowiska testowego i terminów przeprowadzenia testów;
  - Przebieg testów z odniesieniem do punktu 6.2.3;
  - Wyniki testów (zaliczony/niezaliczony z uzasadnieniem);
  - Opis błędów lub nieprawidłowości oraz zalecenia (jeśli dotyczy);

Protokół ten stanowi podstawę do oceny poprawności wykonania oraz odbioru etapu wdrożenia.

#### 9.5. Odbiór Zadania III i IV

- a) Odbiór Zadania IV (Integracja) odbywa się łącznie z odbiorem Zadania III (Wdrożenie).
- b) Podpisanie Protokołu odbioru Zadania III możliwe jest wyłącznie po:
  - pełnym zakończeniu i pozytywnym przetestowaniu wszystkich integracji z systemami z punktu 9.1,
  - potwierdzeniu, że system działa zgodnie z Projektem Technicznym i wymaganiami OPZ.
- c) W przypadku niezaliczenia testów, Wykonawca wprowadza poprawki w ciągu 5 dni roboczych.

## 10. ZADANIE V – OPTIMALIZACJA DZIAŁANIA SYSTEMU SOAR

W ramach Zadania V Wykonawca przeprowadzi optymalizację działania Systemu SOAR, dostosowując jego konfigurację i funkcjonalności do środowiska Zamawiającego oraz bieżących potrzeb operacyjnych zespołu SOC. Działania będą prowadzone zgodnie z harmonogramem realizacji zadań w pkt 5

#### 10.1. Zakres prac optymalizacyjnych

- a) Zaawansowana parametryzacja systemu, obejmująca dostosowanie ustawień, reguł i harmonogramów.
- b) Dostosowanie istniejących integracji i przepływów pracy (workflow) do rzeczywistych procesów operacyjnych.
- c) Optymalizacja oraz rozbudowa playbooków automatyzujących reakcje na incydenty.
- d) Analiza logów, alertów i metryk – identyfikacja oraz eliminacja wąskich gardeł.
- e) Wdrożenie dobrych praktyk oraz rekomendacji producenta i branżowych.

## 10.2. Raportowanie i rozliczenie

- a) Wykonawca przekaże Zamawiającemu miesięczne sprawozdania z wykonanych prac, zawierające:
  - opis zrealizowanych działań,
  - informacje o wykrytych i rozwiązanych problemach,
  - wykaz zmodyfikowanych komponentów (konfiguracje, konektory, reguły),
  - zestawienie opracowanych lub zmienionych playbooków,
  - raport wykorzystanych godzin roboczych.
- b) Zakończenie prac zostanie potwierdzone podpisanym przez obie Strony Protokołem odbioru Zadania V.

## 11. ZADANIE VI - WYKONANIE DOKUMENTACJI POWYKONAWCZEJ SYSTEMU SOAR.

W ramach realizacji Zadania VI, Wykonawca opracuje i dostarczy Zamawiającemu Dokumentację Powykonawczą Systemu SOAR, przygotowaną na podstawie zaakceptowanego przez Zamawiającego Projektu Technicznego. Dokumentacja ma na celu zapewnienie pełnej przejrzystości, audytowalności i możliwości samodzielnego administrowania systemem przez Zamawiającego.

### 11.1. Zakres i struktura dokumentacji

Dokumentacja powykonawcza obejmuje szczegółowy opis wykonanej konfiguracji systemu i składa się z dwóch części:

- a) Dokumentacja podstawowa – zawiera szczegółowy opis wdrożenia,
- b) Załącznik: Dokumentacja administratora – zawiera procedury eksploatacyjne i administracyjne.

### 11.2. Zawartość dokumentacji podstawowej

Dokumentacja podstawowa musi zawierać:

- a) Opis architektury systemu:
  - architekturę logiczną (warstwy: zbieranie, korelacja, automatyzacja, prezentacja),
  - architekturę fizyczną (rozmieszczenie sprzętu, adresacja IP, VLAN-y),
  - schematy przepływu danych między systemami (np. SIEM → SOAR → EDR → SerwisDesk).
- b) Integracje:
  - listę zrealizowanych połączeń z systemami (np. SIEM, EDR, WAF, SerwisDesk, AD),
  - mechanizmy komunikacji i protokoły,
  - mapowanie pól i transformację danych,
  - parametry konfiguracyjne konektorów.
- c) Playbooki i automatyzacja:
  - zestawienie i opis wszystkich wdrożonych playbooków,
  - schematy logiczne przepływu informacji w playbookach (np. diagramy sekwencji, flowcharty),
  - logikę działania, warunki uruchamiania i obsługę błędów.
- d) Bezpieczeństwo i zarządzanie dostępem:
  - konfigurację polityk bezpieczeństwa,
  - opis modelu RBAC, ról i uprawnień,
  - procedury audytu i logowania aktywności użytkowników.
- e) Informacje techniczne:
  - zrzuty ekranów kluczowych elementów konfiguracji (playbooki, integracje, zarządzanie incydentami),

- informacje o wersjach oprogramowania (SOAR, middleware, bazy danych).
- f) Szablony i formaty edytowalne:
- wszystkie zaimplementowane playbooks i scenariusze w formacie edytowalnym (np. YAML, JSON),
  - wzory konfiguracji kluczowych komponentów (konektory, reguły korelacyjne).
- g) Scenariusze integracji i automatyzacji
- Wykonawca zobowiązany jest dostarczyć szczegółowe opisy scenariuszy integracji i automatyzacji, obejmujące każdy kluczowy playbook lub grupę powiązanych playbooków. Dokumentacja powinna zawierać co najmniej: cel scenariusza (np. izolacja hosta, analiza IOC, eskalacja incydentu),
- warunki uruchamiania (np. „jeśli typ incydentu = Malware”, „jeśli reputacja IP = malicious”),
  - źródła danych wejściowych (systemy, formaty danych, częstotliwość),
  - przepływ danych i akcji (opis kroków, systemy angażowane, mapowanie pól, akcje),
  - oczekiwany rezultat (np. utworzenie incydentu w SerwisDesk, dodanie hosta do listy izolowanych w CMDB, wysłanie raportu do SOC),
  - częstotliwość uruchamiania (szacunkowa liczba uruchomień dziennie/tygodniowo),
  - wymagania jakościowe (maksymalny czas wykonania, obsługa błędów, logowanie akcji, mechanizmy monitorowania poprawności),
  - przykładowe dane testowe (opcjonalnie, w formie zanonimizowanego payloadu).

#### 11.3. Załącznik: Dokumentacja administratora

Jako załącznik do dokumentacji podstawowej Wykonawca dostarczy „Dokumentację administratora”, zawierającą:

- a) procedury administracyjne, w tym aktualizacji oprogramowania, playbooków i integracji,
- b) metody i narzędzia diagnostyczne do weryfikacji działania systemu,
- c) procedury wykonywania i weryfikacji kopii zapasowych (wraz z harmonogramem),
- d) procedury kontrolowanego uruchamiania i wyłączania komponentów,
- e) procedurę przywracania systemu z kopii zapasowej (aplikacje + dane),
- f) opis procesów operacyjnych (cykl życia incydentu, eskalacja, zarządzanie playbookami).

#### 11.4. Wymagania formalne i szczegółowość

- a) język: polski,
- b) struktura: spis treści, metryka dokumentu (numer umowy, kierownik projektu, wersja, data, status),
- c) format: dostarczona w wersji edytowalnej (.docx) i PDF, EA.

#### 11.5. Procedura odbioru dokumentacji:

- a) Wykonawca prześle dokumentację w wersji elektronicznej do akceptacji nie później niż 7 dni przed terminem
- b) Zamawiający w ciągu 2 dni roboczych zgłosi uwagi.
- c) Wykonawca wprowadzi zgłoszone uwagi w terminie do 3 dni od ich otrzymania.
- d) Po poprawkach Zamawiający ponownie dokona weryfikacji w terminie 2 dni roboczych.
- e) Komunikacja dotycząca akceptacji dokumentacji będzie prowadzona mailowo, na adresy wskazane w umowie.
- f) Zatwierdzoną dokumentację Wykonawca prześle najpóźniej w dniu podpisania Protokołu odbioru Zadania VI w dwóch wersjach elektronicznych (na pendrive, w wersji edytowalnej i PDF),
- g) Potwierdzeniem wykonania Dokumentacji Powykonawczej będzie podpisany z wynikiem pozytywnym Protokół odbioru Zadania VI.

## 12. ZADANIE VII – PRZEPROWADZENIE INSTRUKTAŻU (WARSZTATÓW)

### 12.1. Zakres zadania

Wykonawca przeprowadzi instruktaż, obejmujący:

- a) Opracowanie materiałów szkoleniowych – w języku polskim, w formacie PDF, zawierających część teoretyczną i praktyczną. Materiały zostaną udostępnione uczestnikom najpóźniej w dniu rozpoczęcia danej edycji.
- b) Organizację i realizację dwóch edycji instruktażu – każda dla co najmniej 4 osób, łącznie dla minimum 8 uczestników. Każda edycja potrwa co najmniej 3 dni i obejmie 24 godziny lekcyjne (po 45 minut).
- c) Dwa poziomy warsztatów:
  - c1) Poziom podstawowy – dla użytkowników końcowych (min. 8 osób, w tym co najmniej 4 z zespołu SOC). Zakres: obsługa GUI, tworzenie i edycja playbooków, integracje, analiza incydentów i raportowanie.
  - c2) Poziom zaawansowany – dla administratorów (min. 2 osoby z zespołu SOC). Zakres: zarządzanie uprawnieniami (RBAC), konfiguracja systemu, procedury backupu i recovery, zaawansowane zarządzanie playbookami i integracjami.
- d) Opracowanie sprawozdania z instruktażu – na podstawie elektronicznych arkuszy AIOS (Ankieta Indywidualnej Oceny Szkolenia) wypełnionych przez uczestników.

### 12.2. Tematyka instruktażu

Zakres tematyczny obejmuje:

- a) Podstawy systemu SOAR:
- b) Rola systemu, integracje z innymi narzędziami, interfejs użytkownika, struktura danych, kluczowe pojęcia, korelacja alertów, powiadomienia, budowa akcji i przegląd modułów.
- c) Administracja systemem:
- d) Architektura, integracje (SIEM, AD, EDR, itp.), tworzenie playbooków, monitoring, rozwiązywanie problemów, RBAC, backup i recovery.
- e) Automatyzacja i Orkiestracja:
- f) Zasady i ograniczenia automatyzacji, logika playbooków, tryby uruchamiania, obsługa błędów, integracje, ćwiczenia praktyczne.
- g) Zarządzanie incydentami:
- h) Obsługa incydentów, automatyzacja triage'u, klasyfikacja, przykładowe scenariusze (np. phishing), raportowanie i metryki (MTTD, MTTR, SLA).
- i) Threat Intelligence (TIP):
- j) Funkcjonalność modułu, dane IOC/IOA, korelacja, automatyczne reakcje, integracja z regułami i playbookami.
- k) Raportowanie i dashboardy:
- l) Gotowe raporty i KPI, tworzenie i edycja, eksport danych, analiza automatyzacji.

### 12.3. Warunki realizacji

- a) Instruktaż zostanie przeprowadzony w terminie do 24 tygodni do dnia odbioru Zadania VI – nie dłużej niż 24 tygodni od dnia zawarcia umowy, zgodnie z harmonogramem realizacji zadań określonym w punkcie 5
- b) Instruktaż odbędzie się zdalnie, z dostępem do wdrożonego systemu lub inną formą uzgodnioną z Zamawiającym. Wykonawca zapewni odpowiednie rozwiązania techniczne.
- c) Zajęcia poprowadzą trenerzy posiadający certyfikaty producenta systemu oraz minimum 3-letnie doświadczenie w pracy z rozwiązaniami SOAR.

### 12.4. Ocena i dokumentacja

- a) Na początku każdej edycji uczestnicy zostaną poinformowani o obowiązku wypełnienia arkusza AIOS po zakończeniu szkolenia.



- b) Po zakończeniu każdy uczestnik otrzyma arkusz AIOS drogą elektroniczną.
- c) Na podstawie zebranych ocen Wykonawca opracuje zbiorczą analizę satysfakcji i użyteczności, którą przekaże Zamawiającemu w ciągu 2 dni roboczych.
- d) W przypadku negatywnej oceny (średnia ocena trenera poniżej 3) lub niezgodności z wymaganiami, Wykonawca zorganizuje dodatkową edycję szkolenia – na własny koszt, nie później niż 10 dni przed zakończeniem terminu realizacji Zadania VII.

#### 12.5. Zaświadczenia

- Wykonawca wystawi imienne zaświadczenia zawierające: imię i nazwisko, tytuł szkolenia, liczbę godzin, tematykę, datę oraz podpis prowadzącego.
- Warunkiem otrzymania zaświadczenia jest: obecność na wszystkich dniach instruktażu (potwierdzona logowaniem) oraz wypełnienie arkusza AIOS.

#### 12.6. Dokumentacja i odbiór

- a) W ciągu 2 dni roboczych po zakończeniu każdej edycji Wykonawca przekaże Zamawiającemu:
  - zeskanowane arkusze AIOS (PDF),
  - potwierdzenie obecności uczestników każdego dnia (printscreen z platformy zdalnej).
- b) Każda edycja zostanie odebrana na podstawie Protokołu odbioru podpisanego przez upoważnione osoby ze strony Wykonawcy i Zamawiającego.
- c) W ciągu 4 dni roboczych od zakończenia edycji, Wykonawca dostarczy papierowy Protokół odbioru instruktażu.
- d) Zakończenie Zadania VII zostanie potwierdzone podpisanym Protokołem odbioru,

### 13. ZADANIE VIII – GWARANCJA I ASYSTA TECHNICZNA

Wykonawca zobowiązany jest do świadczenia usług gwarancyjnych oraz asysty technicznej przez okres 36 miesięcy od daty podpisania z wynikiem pozytywnym Częściowego Protokołu Odbioru dla zadania V. Gwarancją objęty jest cały zbudowany system jako całość (zarówno sprzęt, jak i oprogramowanie, konfiguracje, integracje).

W ramach realizacji niniejszego zobowiązania zapewnione zostaną:

- gwarancja na sprzęt i system jako całość,
- wsparcie producenta systemu SOAR (w zakresie aktualizacji, poprawek, konsultacji),
- asysta techniczna Wykonawcy w zakresie utrzymania i dostosowywania systemu.

Poniżej określono szczegółowe zasady realizacji poszczególnych świadczeń.

#### 13.1. Gwarancja producenta sprzętu

- a) Wszystkie komponenty sprzętowe objęte przedmiotem zamówienia, dla których producent przewidział gwarancję, muszą być dostarczone z ważną gwarancją producenta obowiązującą przez co najmniej 36 miesięcy.
- b) Wykonawca nie może ograniczyć lub wyłączyć gwarancji producenta; gwarancje te obowiązują niezależnie od gwarancji wykonawcy.
- c) W przypadku awarii sprzętu, Wykonawca zobowiązany jest do realizacji procedury gwarancyjnej producenta oraz zapewnienia wymiany sprzętu lub dysków na wolne od wad w ciągu 3 dni roboczych od rozpoczęcia działań diagnostycznych. Uszkodzone dyski przechodzą na własność Zamawiającego.

#### 13.2. Gwarancja wykonawcy na cały wdrożony system SOAR:

Wykonawca udzieli nieodpłatnej gwarancji na cały wdrożony System SOAR oraz wszystkie jego komponenty – w tym elementy nieobjęte gwarancją producenta (np. oprogramowanie autorskie, komponenty Open Source, konfiguracje, integracje) – na okres co najmniej 36 miesięcy, liczony od dnia podpisania z wynikiem pozytywnym Częściowego Protokołu Odbioru dla zadania V.

#### 13.3. Wsparcie producenta oprogramowania Systemu SOAR w okresie gwarancji

W okresie gwarancji wykonawca zapewni Zamawiającemu wsparcie producenta Systemu SOAR, obejmujące co najmniej:

- a) dostarczanie i instalacje nowych wersji oprogramowania oraz poprawek bezpieczeństwa udostępnianych przez producenta,
- b) przeprowadzenie co najmniej raz na 6 miesięcy przeglądu systemu, obejmującego ocenę jego konfiguracji, wydajności i zgodności z zaleceniami producenta.
- c) konsultacje techniczne w ramach trzeciej linii wsparcia producenta.

#### 13.4. Obsługa problemów w okresie gwarancji – SLA

W okresie gwarancji Wykonawca zapewni obsługę zgłoszonych przez Zamawiającego problemów z funkcjonowaniem Systemu SOAR, zgodnie z poniższymi warunkami SLA:

Kategoria problemu	Czas reakcji	Czas przywrócenia (rozwiązanie tymczasowe/ostateczne)	Czas naprawy (rozwiązanie końcowe)
Awaria krytyczna (P1)	6	24h	3 dni
Błąd istotny (P2)	8	48h	4 dni
Błąd niekrytyczny (P3)	2 dni	wg uzgodnień	Kolejne wydanie systemu / poprawka planowa

Podane dni i godziny dotyczą godzin i dni roboczych.

##### 13.4.1. Definicje:

- a) Awaria krytyczna (P1) – całkowita utrata działania kluczowego komponentu systemu, np. brak dostępu do interfejsu SOAR, przestój orchestratora lub bazy danych, brak przetwarzania alertów z SIEM przez ponad 15 minut.
- b) Błąd istotny (P2) – częściowa awaria systemu ograniczająca funkcjonalność, bez całkowitej utraty działania, np. problemy z integracją jednego z systemów bezpieczeństwa, opóźnienia w wykonywaniu playbooków.
- c) Błąd niekrytyczny (P3) – problem o niewielkim wpływie na pracę SOC, bez wpływu na ciągłość działania IT, np. błędy interfejsu, niepoprawne komunikaty, drobne usterki wizualne.
- d) Czas reakcji – maksymalny czas od momentu zgłoszenia do rozpoczęcia działań diagnostycznych.
- e) Czas przywrócenia – czas na wdrożenie rozwiązania tymczasowego lub docelowego, umożliwiającego dalszą pracę systemu,
- f) Czas naprawy – czas całkowitego usunięcia problemu i przywrócenia pełnej funkcjonalności.
- g) Zastosowanie rozwiązania zastępczego nie zwalnia Wykonawcy z obowiązku wdrożenia rozwiązania końcowego.

#### 13.4.2. Kanały zgłoszeń

Problemy można zgłaszać 24/7, przez:

- a) infolinię telefoniczną (bez dodatkowych opłat),
- b) dedykowaną stronę internetową lub system zgłoszeniowy online,
- c) pocztę elektroniczną.

#### 13.4.3. Realizacja zgłoszeń:

Ryzyko nieodebrania zgłoszenia spoczywa na Wykonawcy.

#### 13.4.4. Dodatkowe warunki

- a) Dla awarii krytycznych (P1) Wykonawca zapewnia:
  - możliwość zdalnej interwencji natychmiastowej,
  - interwencję on-site.
- b) W przypadku powtarzających się incydentów tego samego typu (min. 3 razy w ciągu 6 miesięcy), Wykonawca zobowiązany jest do:
  - przeprowadzenia analizy przyczyn źródłowych (RCA – Root Cause Analysis),
  - opracowania i przekazania Zamawiającemu raportu RCA z zaleceniami,
  - wdrożenia działań zapobiegawczych.
- c) SLA obowiązuje bez ograniczeń również w przypadku:
  - komponentów opartych na oprogramowaniu Open Source,
  - autorskich integracji (BYOI),
  - konfiguracji i playbooków dostarczonych przez Wykonawcę.

#### 13.4.5. W przypadku zastosowania komponentów Open Source, Wykonawca:

- a) ponosi pełną odpowiedzialność za ich działanie,
- b) zapewnia pełne wsparcie przez okres gwarancji,
- c) wykonuje audyty poprawek, testy, aktualizacje oraz transfer wiedzy.

#### 13.4.6. W okresie gwarancji Wykonawca będzie:

- a) współpracować z Zamawiającym w analizie raportów, testów i audytów bezpieczeństwa,
- b) wdrażać zalecane zmiany, o ile nie naruszają praw autorskich,
- c) ponosić pełne koszty napraw (części, robocizna, transport),
- d) zapewnia ciągłość działania systemu jako całości, również w zakresie komponentów licencjonowanych i zintegrowanych.

#### 13.4.7. Samodzielne zmiany konfiguracji

Samodzielne zmiany konfiguracji przez przeszkolonych pracowników Zamawiającego nie będą podstawą do utraty gwarancji, o ile nie naruszają architektury systemu lub nie prowadzą do uszkodzenia sprzętu.

### 13.5. Asysta techniczna Wykonawcy

13.5.1. Wykonawca zapewni Zamawiającemu usługę asysty technicznej przez cały okres obowiązywania Umowy (36 miesięcy), polegającą na świadczeniu usług doradczych oraz realizacji prac rozwojowych i konfiguracyjnych, które wykraczają poza standardowy zakres serwisu gwarancyjnego (pkt 13.1-13.4), w tym m.in.:

- a) rekonfiguracji Systemu w zakresie niestanowiącym naprawy wady,
- b) integracji z innymi systemami,
- c) uruchamiania nowych funkcjonalności,
- d) czynności związanych z rozbudową Systemu,
- e) analizy zdarzeń i incydentów,
- f) podłączania nowych źródeł danych (logów),
- g) optymalizacji źródeł danych,
- h) konfigurowania alarmów, korelacji, raportów.

13.5.2. Usługa asysty technicznej świadczona jest w wymiarze:

- a) do 144 godzin w całym okresie 36 miesięcy,
- b) w dni robocze w godzinach 08:00–16:00.

13.5.3. Wnioski o świadczenie asysty technicznej będą przekazywane na adres poczty elektronicznej Wykonawcy wskazany w umowie przez uprawnioną osobę odpowiedzialną za realizację umowy ze strony Zamawiającego. Wniosek powinien zawierać opis potrzeby, oczekiwany zakres prac oraz uzasadnienie, że usługa ta nie stanowi naprawy usterki objętej gwarancją.

13.5.4. Wykonawca może odmówić realizacji usługi, jeśli:

- a) limit godzin asysty technicznej został wyczerpany,
- b) realizacja przekroczyłaby dostępny limit godzin.
- c) zgłoszona potrzeba stanowi usunięcie wady systemu objętej gwarancją wykonawcy (pkt 13.2, 13.4), gwarancją producenta sprzętu (pkt 13.1) lub wsparciem producenta systemu (pkt 13.3); w takim przypadku usługa będzie realizowana bez naliczania godzin z puli asysty technicznej.

13.5.5. Rozliczenie usług:

- a) Usługi asysty technicznej są rozliczane z dokładnością do jednej godziny roboczej, zaokrąglanej w górę.
- b) Wykonawca przedstawia półroczne raporty zawierające:
  - liczbę wykorzystanych godzin w danym kwartale,
  - liczbę godzin pozostałych w puli,
  - szczegółowy opis wykonanych zadań (zadanie, data, czas trwania, osoba wykonująca, efekt).
- c) Raporty są przekazywane Zamawiającemu w ciągu 10 dni roboczych od zakończenia każdego półrocza.
- d) Zamawiający ma prawo do audytu wykorzystania godzin asysty technicznej w zakresie:
  - logów czasu pracy,
  - dokumentacji zadań,
  - komunikacji z Wykonawcą,
  - zgłoszeń i wniosków o świadczenie usługi.
- e) Dane do audytu są udostępniane w formie elektronicznej, w terminie nie dłuższym niż 5 dni roboczych od żądania.

### 13.6. Dodatkowa pula godzin nieodpłatnych asysty technicznej

Wykonawca może, w ramach oferty, przewidzieć dodatkową pulę nieodpłatnych godzin asysty technicznej. Usługi realizowane w ramach tej puli podlegają takim samym zasadom wykonywania i dokumentowania, jak określono w pkt 13.5.