Sygn. akt: KIO 5818/26

WYROK

Warszawa, dnia 18. 03. 2026 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodnicząca: Agata Mikołajczyk

Protokolant: Mikołaj Kraska

po rozpoznaniu na rozprawach w dniu 18 lutego i 13 marca 2026 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 22 grudnia 2025 r. przez Odwołującego: **InfoSoftware Polska Sp. z o.o. z/s w Szczepańcowej** (ul. Przemysłowa 5a 38457 Szczepańcowa) w postępowaniu prowadzonym przez Zamawiającego: **Powiat Żyrardowski ul. Limanowskiego 45 96300 Żyrardów,**

- Uczestnik po stronie Zamawiającego: **TK-MED Sp. z o.o. z/s w Chorzowie** (ul. Działkowa 8, 41-506 Chorzów)

orzeka:

1. Oddala odwołanie;
2. Kosztami postępowania odwoławczego obciąża Odwołującego: **InfoSoftware Polska Sp. z o.o. z/s w Szczepańcowej** (ul. Przemysłowa 5a 38457 Szczepańcowa) i:

2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę **7.500 zł 00 gr** (słownie: siedem tysięcy pięćset złotych zero groszy) uiszczoną przez Odwołującego tytułem wpisu od odwołania oraz koszty postępowania odwoławczego poniesione przez Zamawiającego tytułem wynagrodzenia pełnomocnika w kwocie **3 600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy);

2.2. zasądza od Odwołującego na rzecz Zamawiającego: **Powiat Żyrardowski ul. Limanowskiego 45 96300 Żyrardów** koszty postępowania odwoławczego w kwocie **3 600 zł 00 gr** (słownie: trzy tysiące sześćset złotych zero groszy).

Na orzeczenie - w terminie 14 dni od dnia jego doręczenia - przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie - Sądu Zamówień Publicznych.

……

Sygn. akt: KIO 5818/25

Uzasadnienie

Odwołanie zostało wniesione do Prezesa Krajowej Izby Odwoławczej w dniu 22 grudnia 2025 r. przez wykonawcę InfoSoftware Polska Sp. z o.o. z/s w Szczepańcowej (Odwołujący) w postępowaniu prowadzonym na podstawie ustawy z dnia 11 września 2019 r. - Prawo zamówień publicznych (Dz. U. z 2024 r. poz. 1320 ze zm.), [ustawa Pzp lub Pzp lub Ustawa PZP] w trybie konkursu nieograniczonego, jednoetapowego, realizacyjnego na: „Opracowanie koncepcji architektonicznej szkoły ponadpodstawowej wraz z poradnią psychologiczno-pedagogiczną w Tarczynie” (Konkurs SARP nr 1082) przez Zamawiającego: Powiat Żyrardowski ul. Limanowskiego 45 96300 Żyrardów. Przedmiotem zamówienia jest: „Dostawa i wdrożenie systemu bezpieczeństwa SIEM/SOAR w ramach projektu grantowego „Cyberbezpieczny Samorząd” – Znak sprawy: ZP.272.5.29.2025.). Ogłoszenie nr 2025/BZP 00509036/01).

Wykonawca podał: (…) wnoszę odwołanie od niezgodnych z przepisami PZP czynności i zaniechania dokonania czynności przez Zamawiającego w postaci:

1. odrzucenia oferty Odwołującego jako niezgodnej z warunkami zamówienia w sytuacji, gdy oferta ta jest zgodna z tymi warunkami, a oferowany system spełnia wszystkie wymagania Zamawiającego, a sama ocena intuicyjności rozwiązań jest ocena subiektywną, sprzeczną z ustawą;
2. odrzucenia oferty Odwołującego jako zawierającej rażąco niska cenę w sytuacji, gdy Wykonawca przedstawił wyczerpujące wyjaśnienia potwierdzające, że oferowana cena nie jest rażąco niska;
3. wyboru jako najkorzystniejszej oferty podlegającej odrzuceniu,
4. zaniechania odrzucenia oferty TK-MED. Sp. z o.o. jako niezgodnej z warunkami zamówienia w zakresie zgodności oferowanego systemu z wymaganiami Zamawiającego.

ewentualnie

5. zaniechania unieważnienia postępowania jako obarczonego niemożliwą do usunięcia wadą, która powoduje niemożność zawarcia niepodlegającej unieważnieniu umowy, tj. z uwagi na wewnętrznie sprzeczny i niejednoznaczny opis przedmiotu zamówienia, który nie pozwala na prawidłową ocenę ofert, jak również dający Zamawiającemu prawo subiektywnej oceny niezgodności systemu z jego oczekiwaniami.

Zamawiającemu zarzucam naruszenie:

1)art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) - 3) ustawy Pzp, poprzez bezzasadne odrzucenie oferty Odwołującego jako niezgodnej z warunkami zamówienia, gdy w rzeczywistości oferowany system spełnia wszystkie wymagania określone przez Zamawiającego w OPZ, a ocena intuicyjności rozwiązań jest sprzeczna z ustawą i nieproporcjonalna do zaspokojenia uzasadnionych potrzeb Zamawiającego,

2)art. 226 ust. 1 pkt 8) w zw. z art. 224 ust. 6 ustawy Pzp, poprzez błędne uznanie, że cena oferty Odwołującego jest rażąco niska i niezaakceptowanie wyjaśnień złożonych przez Odwołującego, gdy wyjaśnienia te potwierdzają, że cena nie jest rażąco niska,

3)art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) i 2) ustawy Pzp, poprzez zaniechanie odrzucenia oferty TK-MED Sp. z o.o., gdy zaoferowany przez tego wykonawcę system nie posiada wymaganych opisem przedmiotu zamówienia funkcjonalności,

4)art. 239 ust. 1 i 2 ustawy Pzp, poprzez wybór oferty, która najkorzystniejsza nie jest,

ewentualnie, w przypadku nieuwzględnienia zarzutów 1 lub 2:

5)art. 239 ust. 1 i 2 ustawy Pzp, poprzez wybór oferty sytuacji, w której postępowanie podlega unieważnieniu,

6)art. 255 pkt 6) w zw. z art. 457 ust. 1 pkt 1) w zw. z art. 99 ust. 1 i 4 i w zw. z art. 16 pkt 1) i 2) ustawy Pzp ustawy Pzp, poprzez zaniechanie unieważnienia postepowania w sytuacji, gdy postępowanie to obarczone jest niemożliwą do usunięcia wadą, która powoduje niemożność zawarcia niepodlegającej unieważnieniu umowy, wynikającą z wewnętrznie sprzecznego i niejednoznacznego opisu przedmiotu zamówienia, który nie pozwala na prawidłową ocenę ofert, jak również daje Zamawiającemu prawo subiektywnej oceny niezgodności systemu z jego oczekiwaniami przez pryzmat niezdefiniowanej intuicyjności.

Wskazując na powyższe zarzuty, wnoszę o:

I.uwzględnienie odwołania,

II.nakazanie Zamawiającemu:

a)unieważnienie czynności wyboru oferty najkorzystniejszej,

b)unieważnienie czynności odrzucenia oferty Odwołującego,

c)ponowienie procedury badania i oceny ofert, w tym odrzucenie oferty TK- MED. Sp. z o.o.,a w przypadku uwzględnienia zarzutów ewentualnych

d)unieważnienie postępowania.

Nadto, wnoszę o:

I.(…),

II.dopuszczenie i przeprowadzenie dowodów z dokumentów załączonych do odwołania na okoliczności wskazane w uzasadnieniu odwołania,

III.zobowiązanie Zamawiającego do załączenia dokumentacji postępowania o udzielenie zamówienia, którego dotyczy odwołanie,

IV.zobowiązanie Zamawiającego do wniesienia pisemnej odpowiedzi na odwołanie.

W uzasadnieniu stanowiska wskazał na następujące okoliczności:

I.Interes we wniesieniu odwołania

Zgodnie z art. 505 ust. 1 Pzp środki ochrony prawnej przewidziane w ustawie przysługują podmiotowi, który ma lub miał interes w uzyskaniu danego zamówienia oraz poniósł lub może ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów Pzp. Odwołujący się złożył ofertę w postępowaniu, która zgodnie z informacją z dnia 17 grudnia br. została odrzucona. Oferta Odwołującego była jedyną ofertą złożona poza ofertą, której wyboru dokonał Zamawiający. W ocenie Odwołującego, prawidłowa ocena ofert, nie powinna skutkować odrzuceniem oferty Odwołującego, a powinna prowadzić do odrzucenia oferty TK-MED. Sp. z o.o. Przesłanką legitymacji do wniesienia odwołania jest także możliwość poniesienia szkody w wyniku naruszenia przez Zamawiającego przepisów Pzp. Odwołujący prowadzi działalność gospodarczą, która koncentruje się m.in. wokół dostaw oprogramowania dla jednostek sektora finansów publicznych. Znaczna część zobowiązań Odwołującego, dotyczy kontraktów pozyskanych w wyniku udzielenia zamówienia publicznego. Zainteresowanie Odwołującego uzyskaniem zamówienia będącego przedmiotem postępowania prowadzonego przez Zamawiającego jest zatem związane bezpośrednio z profilem jego działalności. Jakiekolwiek naruszenia po stronie Zamawiającego, które mogą mieć wpływ na końcowy wynik postepowania, w przedmiotowym stanie faktycznym wprost narażają Odwołującego na szkodę i utratę jednego ze źródeł dochodu. W rezultacie, utrzymanie w mocy decyzji Zamawiającego będzie skutkowało uniemożliwieniem Odwołującemu uzyskania

przedmiotowego zamówienia i osiągnięcia oczekiwanego zysku w sytuacji, gdy wybór oferty najkorzystniejszej dokonany został wbrew ustawie. Jednocześnie, nawet w sytuacji oddalenia zarzutów co do bezzasadnego odrzucenia oferty Odwołującego, posiada on interes w żądaniu unieważnienia postępowania. Działania Zamawiającego musza pozostawać transparentne i obiektywne, a pozycja wykonawców równa z perspektywy dostępu do zamówienia i zasad oceny ich świadczeń. Utrzymanie w mocy decyzji o wyborze oferty najkorzystniejszej w świetle zaniechań dotyczących opisu przedmiotu zamówienia będzie prowadziło do uznania, że zamawiający mają prawo do bezrefleksyjnego tworzenia dokumentów zamówienia, a następnie do subiektywnej, niepoddanej żadnej kontroli oceny ofert. W związku z powyższym uznać należy, że Odwołującemu się przysługuje interes do wniesienia niniejszego odwołania.

II.Opis stanu faktycznego

Przedmiotem zamówienia jest dostawa i wdrożenie systemu bezpieczeństwa SIEM/SOAR opisanego w Załączniku nr 8 do SWZ – Opis przedmiotu zamówienia. Zgodnie ze wspomnianym opisem:

(str. 1 Załącznika nr 8 do SWZ)
(str. 2 Załącznika nr 8 do SWZ)

Zgodnie z treścią Opisu przedmiotu zamówienia system musi spełniać powyższe wymagania. A contrario, literalne znaczenie słowa „musi" oznacza, że oferowany system nie może nie posiadać którejkolwiek z wymaganych funkcjonalności. Jednocześnie w dalszej części Opisu przedmiotu zamówienia, Zamawiający zawarł następujący opis:

(str. 21 i 22 Załącznika nr 8 do SWZ)

Zamawiający nie zdefiniował w żaden sposób co i w jaki sposób (w oparciu o jakie kryteria) będzie oceniał pod kątem „intuicyjności". Dodatkowo, Zamawiający w sposób niejasny i sprzeczny z pozostałą treścią Opisu przedmiotu zamówienia opisał zasady oceny „Zgodności". Zgodnie z tym opisem, system może nie posiadać funkcjonalności, co do których Zamawiający napisał wcześniej, że posiadać je musi.

W postępowaniu oferty złożyło dwóch Wykonawców:

Wykonawca TK-MED Sp. z o.o. zaoferował system, którego nie jest producentem. Odwołujący zaoferował własny system IS Sec Scan.

Zamawiający dokonując oceny zaoferowanych systemów, oceniał w zakresie oferty TK-MED Sp. z o.o. m.in. wymagania dotyczące spełniania przez system pkt 11) OPZ (wspomnianego na str. 6 odwołania).

Zgodnie z formularzem oceny, system nie wspiera składni URI, co do której OPZ wskazywał, że funkcjonalność taką musi posiadać.

W pozostałym zakresie Zamawiający nie znalazł brakujących funkcjonalności, a oceniając „Intuicyjność" przyznał niemal w każdym aspekcie maksymalną ocenę.

Dokonując oceny systemu Odwołującego, Zamawiający stwierdził rzekomy brak wielu funkcjonalności oraz negatywnie ocenił „Intuicyjność" większości ocenianych wymagań, opisując m.in.:

− „Wszystkie nazwy po angielsku, brakuje opisów i wyjaśnienia co dana funkcja robi. Istnieje możliwość wyszukiwania po nazwie"

− „Mapa znajduje się w podmenu, posiada wymiary 966x800 na ekranie FullHD, co stanowi 37,3% powierzchni ekranu, a schowanie paska bocznego nie powiększa obrazu. Wykorzystanie monitora o większej rozdzielczości nie zwiększa obszaru roboczego mapy. Tym samym cała mapa jest mała i nieczytelna";

lub podnosząc, że pewnych funkcjonalności nie odnalazł.

Korzystając z uprawnienia wskazanego w pkt 145 lit. g) OPZ, Odwołujący zaproponował spotkanie w formie zdalnej za pomocą platformy Teams, podczas którego odniesie się do wyników ocen zgodności i intuicyjności systemu opracowanych przez Zamawiającego.

W pkt 145 lit. g) nie określono żadnych szczególnych obowiązków związanych ze sposobem odniesienia się do oceny Zamawiającego.

Na spotkaniu 2 grudnia 2025 r. Zamawiający podniósł, że oczekuje prezentacji systemu „na żywo" nie informując o takich planach wcześniej, do czego Odwołujący nie był przygotowany. Mimo to Odwołujący wyjaśnił, że jako producent oprogramowania posiada wiedzę co do tego, że zarzuty stawiane przez Zamawiającego są niezasadne, a system posiada wszelkie wymagane funkcjonalności.

Jednocześnie, z uwagi na wyrażoną przez Zamawiającego potrzebę odbycia prezentacji każdego z wątpliwych wymagań, Odwołujący zaproponował niezwłoczne zorganizowanie dodatkowego spotkania, na którym taka prezentację przeprowadzi zgodnie z życzeniem Zamawiającego. Nagranie było nagrywane.

Mimo wysuniętej propozycji, Zamawiający nie wyraził woli uczestnictwa w takim spotkaniu.

Pismem z 4 grudnia 2025 r. Zamawiający wezwał Wykonawcę do wyjaśnienia, na podstawie art. 224 ust. 1 ustawy pzp, do złożenia wyjaśnień w zakresie ceny „w celu weryfikacji możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów."

Wyjaśnienia te Odwołujący złożył w terminie wskazanym przez Zamawiającego w sposób wyczerpujący, odnosząc się do wszystkich istotnych dla wykonania zamówienia kosztów, w tym kosztów wdrożenia, kosztów prac konfiguracyjnych i programistycznych, kosztów licencji, wsparcia technicznego na okres 12 miesięcy. Jednocześnie Odwołujący przedstawił informacje o założonej rezerwie finansowej i spodziewanym zysku. W wyjaśnieniach przedstawiono także szczegółową metodologię i harmonogram prac, wyjaśnienie w zakresie braku kosztów ukrytych oraz stosowanych rozwiązań technicznych.
Złożone wyjaśnienia były w pełni wystarczające do uznania, że Odwołujący jako producent oferowanego systemu, nie oferuje go po cenie rażąco niskiej.
Mimo podjętych przez Odwołującego działań, Zamawiający w dniu 17 grudnia poinformował o odrzuceniu oferty Odwołującego i wyborze oferty TK-MED Sp. z o.o. jako najkorzystniejszej.
Z decyzją Zamawiającego nie sposób się zgodzić.
III.Analiza prawna - Zarzut nr 1
Zgodnie z art. 226 ust. 1 pkt 5) ustawy Pzp, Zamawiający odrzuca ofertę Wykonawcy, jeżeli jej treść jest niezgodna z warunkami zamówienia. Warunki zamówienia należy rozumieć zgodnie z definicją wyrażoną w art. 7 pkt 29 Pzp, która stanowi, że poprzez warunki zamówienia należy rozumieć warunki, które dotyczą zamówienia lub postępowania o udzielenie zamówienia, wynikające w szczególności z opisu przedmiotu zamówienia, wymagań związanych z realizacją zamówienia, kryteriów oceny ofert, wymagań proceduralnych lub projektowanych postanowień umowy w sprawie zamówienia publicznego.
Zamawiający zarzucił Odwołującemu, że oferowany system IS SEC nie spełnia wymagań i posiada określone błędy powodujące niespełnienie następujących punktów OPZ:1), 11), 23) – wyłącznie w zakresie „intuicyjności", 51) – wyłącznie w zakresie „intuicyjności", 75) – wyłącznie w zakresie „intuicyjności", 87), 122), 125) oraz części wymagań stawianych funkcjonalności dodatkowej.
W tym miejscu należy zauważyć, że niezgodność z warunkami zamówienia może dotyczyć różnych aspektów – np. opisu przedmiotu zamówienia lub wymagań proceduralnych. Każda niezgodność wymaga innego dowodzenia ze strony Zamawiającego. Niezgodność systemu z opisem przedmiotu zamówienia musi być dowiedziona przez Zamawiającego, a nie jedynie domniemana. Zgodnie z wyrokiem KIO 199/24 - Niezgodność oferty z warunkami zamówienia musi być oczywista i niewątpliwa, czyli zamawiający musi mieć pewność co do niezgodności oferty z jego oczekiwaniami, przy czym postanowienia SWZ powinny być jasne i klarowne. (...) Aby możliwe było odrzucenie oferty na podstawie art. 226 ust. 1 pkt 5 p.z.p. niezgodność treści oferty z warunkami zamówienia musi być pewna i oczywista, tym samym nie może to być niezgodność wyinterpretowana z treści niestanowiących pełnych danych o planowanym rozwiązaniu projektowym. Również w wyroki KIO 202/24 Izba uznała, że „odrzucenie oferty wykonawcy na podstawie art. 226 ust. 1 pkt 5 p.z.p. musi nastąpić w razie stwierdzenia niebudzącej wątpliwości sprzeczności oferty wykonawcy z jednoznacznymi postanowieniami, wynikającymi z dokumentów zamówienia."
Tymczasem Zamawiający nie udowodnił, że oferowany system jest niezgodny z opisem przedmiotem zamówienia. Zamawiający jedynie przyjął taką tezę w wyniku wadliwie przeprowadzonej procedury badania próbki, w tym w zakresie uniemożliwienia prezentacji systemu po pierwszym nieudanym spotkaniu, na którym Zamawiający przedstawił oczekiwania wcześniej nie sygnalizowane. Odnosząc się do poszczególnych uwag Zamawiającego należy wyjaśnić jak poniżej:
WADA
Zamawiający w pkt. 1 opisu przedmiotu zamówienia sformułował zakaz stosowania rozwiązań typu open source, w tym expressis verbis wymienił Elastic Security jako niedopuszczalne. Weryfikacja próbki systemu wykazała, że „iS SEC SIEM" realizuje podstawowe mechanizmy właśnie poprzez Elastic Security. Oznacza to, że zaoferowany system stoi w sprzeczności z zakazem zawartym w opisie przedmiotu zamówienia, wymienionym jako przykładowy (por. pkt. 1 opisu przedmiotu zamówienia)." Treść Punktu 1.:
„1) Zamawiający nie dopuszcza rozwiązań z otwartym kodem źródłowym ani rozwiązań darmowych, w tym rozwiązań posiadających płatne opcje wsparcia z darmowym oprogramowaniem jak np. Elastic Security, AlienVault, Wazuh, OSSIM, Snort itp."
WYJAŚNIENIE
Zgłoszona przez Zamawiającego powyższa „wada" systemu jest całkowicie nieuzasadniona. Po pierwsze Zamawiający podczas weryfikacji próbki systemu nie miał możliwości stwierdzić, że System iS Sec realizuje podstawowe mechanizmy przez Elastic Security. W przedstawionej Wykonawcy próbce nie było informacji na temat technologii i silników, z których korzysta System. Aby to sprawdzić Zamawiający musiałby mieć dostęp do kodu źródłowego Systemu iS Sec, lub mieć dostęp do konsoli zarządzającej silnikiem Elastic Search (indeksowa baza danych typu noSQL). Wykonawca nie udostępnił Zamawiającemu kodu źródłowego oraz nie dał dostępów do Elastic Search. Wykonawca w opisie do omawianego punktu przesłanym do Zamawiającego również nie wskazał tej technologii (Elastic Security) tylko

dokładnie wymienił Elastic Search. Wykonawca nie wie na jakiej podstawie zamawiający stwierdził, że system ISSec realizuje podstawowe mechanizmy poprzez Elastic Security. Wykonawca stwierdza, że tego typu zgłoszona „wada" wynika z nieznajomości rozwiązań stosowanych w Systemie iS Sec, oraz rozwiązań i technologii Elastic. Elastic Search i Elastic Security są to różne rozwiązania, stosowane w różnych celach. Elastic Search to indeksowa baza danych, która służy w systemie iS Sec jako kolektor logów, jest to technologia bardzo rozpowszechniona i stosowana nawet przez takich gigantów jak Amazon. Odrzucanie tej technologii jest tożsame z odrzucaniem takich baz danych jak MS SQL Express, czy MySQL stosowanych najczęściej przez różnych producentów. Elastic Security natomiast jest to platforma/system od firmy Elastic bazująca na Elastic Search tak samo jak oferowany przez Wykonawcę System iS Sec.

Wykonawca nie zgadza się również z tym, że omawiany i przedstawiony powyżej punkt 1) z OPZ wyklucza z postępowania system iSSec.

1.Zamawiający nie dopuszcza rozwiązań z otwartym kodem źródłowym

Oferowany system iS Sec nie jest systemem z otwartym kodem źródłowym, nie można nigdzie pobrać jego źródła, a klientom dostarczane są tylko skompilowane rozwiązanie (w sloganie informatycznym tzw. binarki).

2.ani rozwiązań darmowych,

Oferowany system iS Sec nie jest system darmowym i nigdzie nie można go pobrać za darmo. System IS sec posiada własny serwer licencyjny, który pilnuje ilości instalowanych urządzeń końcowych, czy licencji okresowych.

3.w tym rozwiązań posiadających płatne opcje wsparcia z darmowym oprogramowaniem jak np. Elastic Security, AlienVault, Wazuh, OSSIM, Snort itp.

Oferowany system iS Sec nie jest rozwiązaniem posiadającym płatne opcje wspracia z darmowym oprogramowaniem jak np. Elastic Security, AlienVault, Wazuh, OSSIM, Snort itp. Wykonawca nie oferuje Zamawiającemu wdrażania żadnego ze wskazanych tutaj systemów. Wykonawca w ramach realizacji takiego zamówienia, wdraża własny system z jego wszystkimi komponentami. Jest to komercyjny system posiadający autorskie rozwiązania umożliwiające centralne zarządzanie infrastrukturą pod kątem cyberbezpieczeństwa takie jak np. analiza behawioralna UEBA, analiza danych AI (wsparcie w analizie logów, problemów, zagrożeń, anomalii) czy tworzenie scenariuszy automatyzujących reakcje na raportowane incydenty bezpieczeństwa. System wyposażony jest we własne mechanizmy SIEM/SOAR.

Ponadto zapis OPZ odnosi się do rozwiązań jako całości, nie do technologii użytej wewnętrznie.

–„rozwiązania open-source" - chodzi o system oferowany zamawiającemu, nie o frameworki, bazy danych czy silniki.

–„rozwiązania darmowe" - chodzi o system oferowany zamawiającemu, nie o komponenty wewnętrzne.

–„rozwiązania free + paid (jak Elastic Security)" - chodzi o produkty dostępne dla klienta w darmowej wersji podstawowej.

WADA

Zgodnie z pkt. 11 opisu przedmiotu zamówienia, Zamawiający określił sposób realizacji funkcjonalności tworzenia parserów, wymagając, aby odbywało się to poprzez graficzny interfejs. W wyniku weryfikacji próbki systemu Zamawiający stwierdził brak funkcjonalności parsowania logów dla następujących typów składni z poziomu interfejsu użytkownika: a) CEF,

b)LEEF, c) URI, d) XML, e) JSON, f) SYSLOG, g) REGEX.

Opis dostarczony przez Wykonawcę wskazywał na konieczność ich wykonania poza środowiskiem graficznym. Ponadto Zamawiający Ponadto w udostępnionej próbce systemu nie odnaleziono możliwości dalszej normalizacji, zaś opis Wykonawcy nie wskazywał miejsca dostępności tej funkcji.

WYJAŚNIENIE

W odniesieniu do tej „wady" systemu iS Sec wykonawca również całkowicie się nie zgadza ze stwierdzeniami Zamawiającego. Nie prawdą jest, że Wykonawca wskazywał w przesłanym zamawiającemu opisie na konieczność ich wykonania poza środowiskiem graficznym.

Zamawiający otrzymał opis:

„OPD. System wyposażony jest w Moduł analizy logów spełniający powyższe wymagania, module tym możliwe jest wyświetlanie i wyszukiwanie wstępnie sprasowanych/niesparowanych logów z różnych źródeł. W zakładce indeksy użytkownik może utworzyć własny indeks oraz w szczegółach indeksu skopiować/podglądnąć dostęp do niego przez udostępnione API. Ponadto w zakładce „Niestandradowe logi", użytkownik może wskazać lokalizację źródła logów poprzez podanie ścieżki do pliku/plików na wybranym hoście oraz przypisanie ich do utworzonego wcześniej indeksu. Możliwość tworzenia parserów znajduję się w zakładce Parsery i jest dość rozbudowana, a przy użyciu składni GROK umożliwia tworzenie praktycznie dowolnych parserów. System umożliwia dowolne parsowanie wstępne i końcowe. Oraz automatycznie rozpoznaje wymienione formaty.

Scenariusz testowania:

1.Zaloguj się do Systemu ISSec z przeglądarki internetowej.

2.Wybierz Moduł analizy logów

3.Przeglądnij zakładkę „Niestandardowe logi”
4.Przeglądnij zakładkę „Parsery”
5.Przeglądnij zakładkę „indexy”
6.Przeglądnij zakładkę „Zaawansowane wyszukiwanie”
Nigdzie w tym zapisie nie jest napisane, że jest konieczne ich wykonanie poza środowiskiem graficznym. Wykonawca domyśla się, że Zamawiającemu chodziło o stwierdzenie „a przy użyciu składni GROK umożliwia tworzenie praktycznie dowolnych parserów”, tylko że system iS Sec umożliwia tworzenie dowolnych parserów przy użyciu składni GROK (nie całego skryptu) z poziomu GUI. Poniżej zrzuty ekranu z GUI Systemu iS Sec:
(…)
Gdyby Zamawiający znał GUI systemu na pewno odnalazłby te funkcjonalności. Scenariusz testowania mówił o przeglądnięciu tych zakładek, i gdyby testujący nacisnął przycisk „Dodaj parser”, to znalazłby tam wszystkie wymagane w tym punkcie funkcjonalności:
(…)
f) SYSLOG
g) REGEX. Wyrażenia regularne Grok
(…)
Ponadto aby stworzyć np. parser SYSLOG należy dodać źródło danych. Aby to zrobić trzeba mieć dostęp do urządzenia SYSLOG i przekierować logi tego urządzenia po konkretny adres. Gdyby Zamawiający dobrze sprecyzował w jaki sposób będzie wykonywana weryfikacja systemu, to można by jakoś to przygotować. Zamawiający nie posiadający wiedzy o architekturze systemu iS Sec, wiedzy o podstawowych zasadach jego funkcjonowania nie miał możliwości zweryfikowania, czy np. SYSLOG jest parsowany. Bo nie mógł dodać w systemie źródła logów, ponieważ testowanie było wykonywane na infrastrukturze sieciowej udostępnionej przez Wykonawcę, o której Zamawiający nie miał żadnych informacji. Poniżej przykłady sparsowania LEEF i SYSLOG.
Ostatnią „wadą” systemu wskazaną przez Zamawiającego w tym zakresie jest: „Ponadto Zamawiający Ponadto w udostępnionej próbce systemu nie odnaleziono możliwości dalszej normalizacji, zaś opis Wykonawcy nie wskazywał miejsca dostępności tej funkcji.”
Wykonawca w scenariuszu wskazał na przeglądnięcie zakładki Indeksy, w której powyższa funkcjonalność się znajduje. Nieznajomość tego rozwiązania (systemu iS Sec) uniemożliwiła Zamawiającemu naciśnięcie przycisku „Dodaj indeks” lub „Edytuj”, gdzie z powodzeniem odnalazłby opcję dalszej normalizacji/parsownia. Poniżej
przykład parsowania w systemie logów przychodzących w formacie LEEF. Na poniższym rysunku widzimy, że „leefindeks”, który zawiera logi wstępnie sparsowane przez system, będzie dalej parsowany przez „Parser logów”, a następnie przez „parserprezentacj”. W systemie iS Sec istnieje możliwość praktycznie dowolnego zagnieżdżania parserów.
(…)
WADA
Wizualizacja w formie interaktywnej sieci została uznana za spełnioną (wymóg określony w pkt. 23 opisu przedmiotu zamówienia), natomiast w zakresie intuicyjności Zamawiający uznał spełnienie wymogu w wymiarze 15%, uzasadniając to w ten sposób, że mapa znajdująca się w podmenu posiada niezmienne wymiary 966x800 pikseli. Oznacza to tyle, że zaoferowane narzędzie, przy rozdzielczości ekranu FullHD, zajmuje zaledwie 37,3% dostępnej powierzchni ekran. Modyfikacje polegające na schowaniu paska bocznego nie powiększyło obrazu. Zamawiający potwierdził powyższe poprzez wykorzystanie monitora o większej rozdzielczości – czynność nie zwiększyła obszaru roboczego mapy. Tym samym cała mapa pozostała niewielkiego rozmiaru, a przez to nieczytelna.
WYJAŚNIENIE
Wykonawca również nie zgadza się z tą uwagą i uznaję ją za nieuzasadnioną. Po pierwsze w żadnym miejscu w dokumentach dotyczących opisu przedmiotu zamówienia nie było wzmianki na temat wizualizacji mapy, czy formy prezentacji różnych danych. Po drugie rozdzielczość mapy, o której jest mowa może być zmieniona wg. wytycznych zamawiającego w procesie konfiguracji systemu w ramach wdrożenia. Jest to rzecz na tyle prosta, że wykonawca jest wstanie w stosunkowo krótkim czasie skonfigurować system tak, żeby np. ta mapa była wyświetlana w osobnym oknie na całości ekranu. Po trzecie wykonawca nie uważa wcale, że zaimplementowana rozdzielczość omawianej mapy sprawia, że jest ona nieczytelna. Mapa jest interaktywna i pozwala użytkownikowi dobrowolnie przybliżać i oddalać jej elementy, dla przykładu przedstawiono poniżej zrzuty z ekranu. Pierwszy dotyczy wizualizacji mapy bez powiększenia/przybliżania na typowym monitorze 27”, drugi przedstawią tą samą mapę z przybliżeniem i trzeci z jeszcze większym przybliżeniem. Przybliżenie dowolnych elementów na mapie jest bardzo intuicyjne wystarczy „najechać” kursorem myszki na dowolny obszar/element mapy i użyć „scrolla” na mszyce. Tak jak to się robi w większości okien różnych systemów. Chwytając myszką dowolny obszar na mapie można też w dowolny sposób tę

mapę przesuwać i nawet wyrzucić ją całkowicie poza obszar roboczy.
(…)
WADA
W ramach wymogu określonego w pkt. 51 opisu przedmiotu zamówienia: a) Możliwość stosowania sparsowanych pól oraz ich wartości została uznana za spełnioną, natomiast w zakresie intuicyjności Zamawiający uznał spełnienie wymogu w wymiarze 12,50%, uzasadniając to w ten sposób, że względem wszystkich nazw pól użyto języka angielskiego, w systemie brak było opisów i wyjaśnienia działania poszczególnych funkcji, niemniej istniała możliwość wyszukiwania po nazwie. b) Możliwość stosowania atrybutów użytkowników z Active Directory została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru atrybutu użytkownika z AD, a instrukcja nie opisywała takiego przypadku. c) Możliwość stosowania atrybutów komputerów z Active Directory została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru atrybutu komputera z AD, a instrukcja nie opisywała takiego przypadku. d) Możliwość stosowania bazy wskaźników kompromitacji (IOC) została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru IoC, a instrukcja nie opisywała takiego przypadku. e) Możliwość stosowania informacji z elektronicznej dokumentacji została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wybory informacji z elektronicznej dokumentacji, a instrukcja nie opisywała takiego przypadku. f) Możliwość stosowania anomalii w zachowaniu użytkowników (UBA) została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru anomalii w zachowaniu użytkowników, a instrukcja nie opisywała takiego przypadku. g) Możliwość stosowania mali w zachowaniu zasobów (EBA) została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru anomalii w zachowaniu zasobów, a instrukcja nie opisywała takiego przypadku. h) Możliwość stosowania podatności na zasobach została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru podatności na zasobach, a instrukcja nie opisywała takiego przypadku. i) Możliwość stosowania wyników analizy konfiguracji została uznana za niespełnioną, bowiem Zamawiający nie odnalazł możliwości wyboru wyników analizy konfiguracji, a instrukcja nie opisywała takiego przypadku.
WYJAŚNIENIE
Wykonawca nie zgadza się ze wskazaną przez Zamawiającą wadą/usterką. W odniesieniu do powyższych podpunktów, również należy stwierdzić, że Zamawiający dokonał niesprawiedliwej oceny na podstawie braku wiedzy na temat systemu, technologii oraz ogólnej zasady działania tego typu systemów. Ponadto uwaga na temat języka angielskiego jest wręcz absurdalna. System iS Sec jest to system stworzony przez Polskiego producenta, który dbając o intuicyjność systemu używa głównie języka polskiego. Dodanie reguł korelacyjnych w systemie odbywa się poprzez wejście w Moduł wykrywania zagrożeń i wybranie zakładki reguły korelacyjne i naciśnięcie przycisku dodaj regułę. Poniżej przedstawiono formularz dodawanie reguły i jest on całkowicie stworzony w języku polskim. Jeśli chodzi o używanie sparsowanych pól w tych regułach, to zależy od użytkownika czy dane pole jest w języku angielskim, czy polskim. Ponadto w dziedzinie IT powszechnie stosuje się język angielski, i każdy wykształcony informatyk wie, czego dotyczy słowo „hostname", „eventlog", czy „winlog". Generalnie zarówno logi jak i informacje dotyczące różnych pól pochodzących z systemów powszechnie stosowanych sprasowane są w systemie w taki sposób aby można było się domyślić z jakich systemów pochodzą. Dla przykładu z MS Office 365 (nie używamy MS Biuro 365) umieszczone w systemie są w indeksie „logs-o365", a pola sparsowane posiadają przedrostek o365. W systemie istnieje możliwość ponownego parsowania dowolnych indeksów, gdzie użytkownik może zmienić nazwy tych pól na dowolne, ale informatyk/administrator, który nie wie co znajduje się np. pod polem, „winlog.process.pid", nie powinien pracować przy tak trudnych zagadnieniach jak cyberbezpieczeństwo.
(…)
Podobna jest sytuacja dla Matrycy Mitre ATT&CK powszechnie stosowanej w systemach klasy SIEM. Jest ona pobierana i oficjalnych źródeł, z których wszyscy producenci na całym świecie korzystają. Taktyki i techniki działania cyberprzestępców są dodawane do tej właśnie matrycy i odpowiednio kategoryzowane. Sprawa jest prosta jest to po Angielsku ponieważ jest to język międzynarodowy, a w IT język ten jest powszechne stosowany i używany we wszelkich dokumentacjach technicznych. Dla przykładu na poniższym zrzucie z systemu przedstawiono wybrany z matrycy rodzaj ataku: „Brute Force" – każdy wykształcony informatyk słyszał o taki zagrożeniu. Następnie mamy listę zaimplementowanych reguł korelacyjny i tak dla przykładu: w tych regułach od razu widać czego dotyczą np. AWS to wiemy że to ten typ chmury, Azure inny itd. itp. jeśli mamy np. Multiple Logon Failure – to znaczy że reguła dotyczy wielokrotnie błędnego wpisania hasła. Informatyk/administrator musi znać te pojęcia, ponieważ większość systemów zagranicznych dostawców, logi wypisuje w języku angielskim, jeśli ktoś nie zna tych podstawowych pojęć nie będzie mógł skutecznie analizować logów z własnej infrastruktury sieciowej i własnych systemów. Większość naszych klientów miałoby wręcz problem z tym, że takie informacje spolszczyliśmy i oni teraz nie mogą się odnaleźć.
(…)
Ponadto system wyposażony jest w odrębny moduł UEBA, moduł wskaźników kompromitacji IoC, itd. i posiada wszystkie

funkcjonalności opisane w powyższych podpunktach, lecz niechęć sprawdzenia (przeklikania systemu) oraz brak wiedzy na jego temat oraz tego typu technologii i systemów uniemożliwił Zamawiającemu odnalezienie tych funkcjonalności. Tak samo jest z opisami reguł, które można znaleźć w listach referencyjnych pod linkiem umieszonym przy każdym zagrożeniu uwzględnionym w Matrycy Mitre ATT&CK.

WADA

Wymóg określony w punkcie 72 opisu przedmiotu zamówienia został uznany za niespełniony, bowiem system nie umożliwiał automatycznego przypisywania zdarzeń do operatora.

WYJAŚNIENIE

Wykonawca nie zgadza się z tą uwagą/usterką, System iS Sec posiada funkcjonalność automatycznego przypisywania zdarzeń do operatorów. Wykonawca opisał ten mechanizm Zamawiającemu i wskazał miejsca konfiguracji. Nieznajomość systemu, technologii oraz działania tego typów systemów uniemożliwiła Zamawiającemu sprawdzenie jak działa ta funkcjonalność. Po pierwsze Zamawiający na próbce systemu otrzymał dostęp do jednego konta (operatora), do którego automatycznie system przypisał wszystkie zdarzenia/incydenty w celu przedstawienia funkcjonalności. Ograniczenie w tym przypadku zdarzeń do innego operatora skutkowałoby brakiem dostępu do tych zdarzeń dla tego operatora (czyli konta które otrzymał Zamawiający). Skutkowałoby to stwierdzeniem przez Zamawiającego, że na przykład w systemie nie ma incydentów dotyczących podatności, co nie jest zgodne z prawdą. Automatyczne przypisanie to znaczy, że coś zostało zrobione bez ingerencji użytkownika. W jaki sposób Zamawiający sprawdził, że tej funkcji niema w systemie, skoro wykonała się ona automatycznie, to jest nadal zagadką. Właśnie sam fakt zalogowania się do systemu jako operator wskazywał Zamawiającemu, że jeśli ma dostęp to automatycznie zostały do niego przypisane wszystkie incydenty. W systemie iS Sec znajduje się kilka możliwości przypisujących konkretne zdarzenia do konkretnych osób/opertorów. Można to robić na kilka sposobów, a jeden z nich przedstawiono Zamawiającemu. Poprzez np. uprawnienia, operatorowi można przyznać dostęp zarówno do sekcji/funkcjonalności jak i grup zasobów. Jeśli podzielimy dostępy zarówno do sekcji systemu jak i zasobów na poszczególnych operatorów, to możemy zapewnić automatyczne przypisanie wszystkich zdarzeń dotyczących podatności CVE na grupie urządzeń SERWERY do konkretnej osoby, która dostaje takie uprawnienia. Mało tego można te uprawnienia w systemie mieszać i użytkownicy o tych samych uprawnieniach dostaną przypisane do siebie te same zdarzenia. W tym momencie użytkownik może ręcznie przypisać operatora i wskazać tą osobę lub przypisać siebie, żeby np. drugi użytkownik wiedział, ze ktoś już zajmuje się tym zdarzeniem. Kolejna opcja to przypisywanie powiadomień do konkretnych operatorów poprzez konfigurację SLA. System wyposażony jest w rozbudowany moduł powiadomień o incydentach i pozwala na tworzenie własnych reguł, w których można ustawić np. zgłoś powiadomienie OPERATOROWI A jeśli jest Incydent jest krytyczny. A jeśli incydent ma priorytet niski to zgłoś OPERATOROWI B. Poniżej przedstawiono zrzuty ekranu z systemu.

Ponadto istnieje jeszcze możliwość z skorzystania z Modułu SOAR, w którym wykrycie konkretnego np. typu zagrożenia można przypisać do konkretnych osób/operatorów i ich powiadomić o tym incydencie.

WADA

Możliwość manualnego grupowania zdarzeń została uznana za spełnioną (wymóg określony w pkt. 75 opisu przedmiotu zamówienia), natomiast Zamawiający uznał rozwiązanie jako nieintuicyjne (0%), uzasadniając to w ten sposób, że wymogiem było przepisanie numeru zdarzenia, który ma łącznie 32 cyfry w formacie heksadecymalnym połączone w pięć grup. System nie posiada możliwości wyszukania po części numeru. Ponadto sama nazwa funkcji nie wskazuje w żaden sposób, że służy do grupowania zdarzeń.

WYJAŚNIENIE

Wykonawca nie zgadza się z tą usterką oraz opinią na temat intuicyjności. Sprawę intuicyjności omówiliśmy już powyżej i nasze stanowisko jest takie, że została ona wykonana nie rzetelnie. Ponadto w punkcie 75 OPZ nie ma opisu w jaki sposób ma się to odbywać. W naszej ocenie aby zgrupować np. dwa zdarzenia należy do jednego zdarzenia przypisać drugie zdarzenie. Dlatego w systemie umieszczono przycisk o nazwie „przypisz zdarzenie”. Po przypisaniu zdarzenia w systemie widzimy zgrupowane zdarzenia. Omawianą sytuacje przedstawiają poniższe zrzuty ekranu.

(…)

Jeśli Zamawiającemu nie przypadła do gustu nazwa tej funkcji to na etapie wdrożenia Wykonawca może skonfigurować system tak aby była inna, choć w naszej ocenia przypisanie zdarzenia jest bardziej intuicyjne.

WADA

W ramach wymogu określonego w pkt. 87 opisu przedmiotu zamówienia: a) Możliwość filtrowania po wyliczonym priorytecie podatności została uznana za niespełnioną, bowiem nie została przewidziana w systemie ani przekazanej instrukcji. b) Możliwość filtrowania po ważności zasobu na którym została wykryta została uznana za niespełnioną, bowiem nie została przewidziana w systemie ani przekazanej instrukcji. c) Możliwość filtrowania po adresie IP tego systemu została uznana za niespełnioną, bowiem nie została przewidziana w systemie ani przekazanej instrukcji. d) Możliwość filtrowania po parametrach SLA związanych z tym statusem została uznana za niespełnioną, bowiem nie

została przewidziana w systemie ani przekazanej instrukcji. e) Możliwość filtrowania po przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe została uznana za niespełnioną, bowiem nie została przewidziana w systemie ani przekazanej instrukcji. f) Możliwość filtrowania po parametrach CVSS, np.: lista podatności których „Access Complexity (AC)" = „low" oraz „Access Vector (AV) = „Network", została uznana za niespełnioną, bowiem nie została przewidziana w systemie ani przekazanej instrukcji.

WYJAŚNIENIE

Wykonawca nie zgadza się z tą uwagą/wadą systemu. Zamawiający dostał do dyspozycji próbkę systemu oraz podstawowy scenariusz testowania. Niestety nie do końca wykonał te proste polecenia albo z jakiś niewyjaśnionych przyczyn nie widział zaawansowanej wyszukiwarki podatności CVE.

„ODP. W systemie ISSec – każda obsługiwana podatność może być wyszukiwana wg. parametrów wypisanych powyżej. System wyposażony jest w zaawansowaną wyszukiwarkę umożliwiającą również wyszukiwanie po kategorii oraz podanej frazy.

Scenariusz testowania:

1.Zaloguj się do Systemu ISSec z przeglądarki internetowej.

2.Wybierz i przeglądnij Moduł SLA

3.Wybierz zakładkę „Podatności"

4.Wybierz incydent i naciśnij przycis „…" (akcje) i wybierz wyświetl CVE

5.Sprawdź możliwości filtrowania wyników"

Konsekwentne wykonanie tego scenariusza i zaznajomienie się z tak prostym opisem, powinno doświadczonego użytkownika tego typu systemów doprowadzić do zupełnie innych wniosków. System wyposażony jest w intuicyjną wyszukiwarkę znajdującą się po prawej stronie podpisaną „wyszukaj", która wyszukuje po podanej frazie, czyli również po IP. Ponadto z lewej strony moduł analizy podatności wyposażony jest w różne filtry wymagane w tym punkcie. Zamawiający nie wykonał piątego punktu z tego scenariusza. System wyposażony jest również w interaktywne wykresy umożliwiające filtrowanie po priorytetach. Kliknięcie w dany „kolor" priorytetu powoduje odfiltrowanie podatności.

Poniżej przedstawiono z rzuty ekranu z systemu.

(…)

WADA

W ramach wymogu określonego w pkt. 122 opisu przedmiotu zamówienia: a) Aplikacja typu agent została uznana za spełnioną, natomiast Zamawiający uznał rozwiązanie jako nieintuicyjne (0%), uzasadniając to w ten sposób, że opis agentów przedstawiony przez Wykonawcę okazał niezrozumiały: w playbookach SOAR nie brak było możliwości zarządzania, instalacji czy zbierania logów z agentów. Ponadto w systemie testowym nie stwierdzono śladów wykorzystania aplikacji typu agent. b) Brak możliwość centralnego zarządzania, a dostarczona instrukcja milczy na temat dostępności. c) Brak możliwość aktualizacji z głównej konsoli zarządzającej, a dostarczona instrukcja milczy na temat dostępności. d) Brak możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows, a dostarczona instrukcja milczy na temat dostępności. e) Brak możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security, System, Application, a dostarczona instrukcja milczy na temat dostępności. f) Brak możliwość monitorowania integralności plików, a dostarczona instrukcja milczy na temat dostępności. g) Brak możliwość monitorowania rejestru systemowego, a dostarczona instrukcja milczy na temat dostępności. h) Brak możliwość monitorowania urządzeń zewnętrznych (removable devices), a dostarczona instrukcja milczy na temat dostępności. i) Odnośnie wymogu komunikowania się agenta w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS Wykonawca oświadczył, że dane są szyfrowane, niemniej nie przedstawił żadnych dowodów. W systemie nie stwierdzono żadnych dedykowanych ustawień, brak był również przechwycenia pakietów sieciowych w celu analizy. j) Brak możliwość monitorowania stanu agentów w konsoli zarządzającej systemu, a dostarczona instrukcja milczy na temat dostępności. k) Brak możliwość przygotowania różnych zestawów konfiguracji agenta, a dostarczona instrukcja milczy na temat dostępności.

WYJAŚNIENIE

Wykonawca nie zgadza się z tą opinią i temat oceny intuicyjności był już poruszany wcześniej. Zamawiający otrzymał od Wykonawcy wyczerpującą odpowiedź i tylko nieznajomość tego typu systemów może doprowadzić do tak skrajnie niesprawiedliwej oceny.

Przekazana odpowiedź:

„ODP. System ISSec może gromadzić logi agentowo i bezagnetowo. System posiada agentów zarówno na Windows jak i na systemy Linux, połączenia agentowe są szyfrowane. Agenci automatycznie zbierają informacje na temat oprogramowania oraz zasobów. Centralne zarządzanie agentami jest możliwe w formie uproszczonej tj. poprzez sprawdzenie ich statusów bądź możliwość ich usuwania. Agenci mają możliwość wykonywania dowolnych skryptów czy reakcji na zgłaszane incydenty takie jak blokada procesu stworzenie dump blokowanie ruchu sieciowego i wiele innych.

Instalowanie agentów może odbywać się ręcznie bądź na systemach Windows przy wykorzystaniu GPO. Wykonawca zapewnia dostęp do plików konfiguracyjnych agentów instrukcji instalacji oraz instrukcji zmiany wybranych parametrów. Wykonawca dostarcza również różne zestawy agentów na Systemy Windows w postaci paczek instalacyjnych MSI.
Scenariusz testowania:
1.Zaloguj się do Systemu ISSec z przeglądarki internetowej.
2.Wybierz moduł SOAR
3.Wybierz zakładkę „Playbooki"
4.Wybierz dodaj playbook
5.Rozwiń zakładkę Skrypty „
W pierwszej kolejności trzeba rozumieć czym jest agent i gdzie on jest instalowany. Agentów nie instaluje się w konsoli Systemu iS Sec, tylko na tkzw. końcówka, czyli urządzeniach końcowych takich jak serwery fizyczne, serwery virtualne desktopy pracowników, laptopy itp. , i podczas ich instalacji agencji rejestrowani są w systemie iS Sec. Wykonawca założył, że sprawdzający tę funkcjonalność jest osoba związaną z środowiskiem IT i wie jak działają systemy agentowe i również wie, że bez agenta zainstalowanego na końcówce nie da się wykonać zdalnie skryptu bez wcześniejszego nawiązania z tym komputerem połączenia np. ssh, rdp itp. Co do szyfrowania , to już sama próbka systemu była udostępniona Zamawiającemu po HTTPS (czyli z użyciem certyfikatu SSL), co może sugerować, że całe rozwiązanie jest szyfrowane. Stan agentów również jest dostępny w zakładce Agneci w Module inwentaryzacji i gdyby wykonawca bez uprzedzeń zapoznał się z próbką nie mógł by tej opcji nie zauważyć.
(…)
Co do dowodów na temat szyfrowania połączeń pomiędzy agentami, a kolektorami logów to Wykonawca bez problemu mógłby je przedstawić, gdyby znał formę oceny intuicyjności na etapie ogłoszenia przetargu.
WADA
W ramach wymogu określonego w pkt. 125 opisu przedmiotu zamówienia: a) Brak możliwość integracji z Threat Inteligence Feed: Zamawiający nie odnalazł opcji umożliwiającej włączenie integracji. Funkcja określona przez Zamawiającego zawierała wyłącznie listę 10 plików zablokowanych. System nie posiadał możliwości integracji z jakimkolwiek systemem Threat Intelligence. b) System nie spełniał wymogi dotyczącego zintegrowanej bazy zagrożeń. Udostępniona baza danych zawierała tylko 10 plików, spośród których 5 w nazwie miało słowo test lub testowy. Dwa pliki to litery leżące bezpośrednio w swoim towarzystwie na klawiaturze, a pozostałe trzy pliki mają tylko liczbę heksadecymalną zamiast nazwy. Hash trzech ostatnich jest identyczny. Udostępniona baza nie zasługiwała na miano bazy danych, lecz były to przykładowe wpisy do bazy danych. W zakresie zadeklarowanej funkcjonalności opcjonalnej nr 2,
WYJAŚNIENIE
Zamawiający całkowicie nie zgadza się z opinia w tym punkcie. Zamawiający chyba w ogóle nie sprawdził co znajduje się w „Module Threat Intelligence". W tym przypadku dla Wykonawcy sprawa była tak oczywista, że Zamawiający otrzymał taką odpowiedź w raz ze scenariuszem do próbki:
„ODP. System jest zintegrowany z zewnętrznymi bazami danych Threat Inteligence.
Scenariusz testowania:
1.Zaloguj się do Systemu ISSec z przeglądarki internetowej.
2.Wybierz z menu Moduł Threat Inteliligence
3.Przeglądnij baze wiedzy z różnych kategorii danych
4.Sprawdź listę blokowanych plików"
Ciężko jest się odnieść do tego zarzutu, Zamawiający w ocenie Wykonawcy nie wykonał scenariusza punkt 2 i 3 wskazuje dokładnie na zintegrowane bazy wiedzy na temat wskaźników kompromitacji. Ponownie Wykonawca uważa, że Zamawiający z przyczyn braku wiedzy na temat tego typu rozwiązań oraz ogólnej niechęci, nieprawidłowo ocenił funkcjonalności systemu iS Sec.
(…)
Co do punktów 10, 11, 12 , 13, 14, 15 dotyczących zadeklarowanej funkcjonalności opcjonalnej, również Wykonawca nie zgadza się z ustaleniami Zamawiającego. Wykonawca przedstawił zamawiającemu scenariusz, którego rzetelne przejście wskazywałoby na zupełnie inną, sprawiedliwą ocenę. System iS Sec jest rozbudowanym system posiadającym te wszystkie funkcjonalności. Wykonawca nie wie dlaczego tak został oceniony, ale podejrzewa albo znaczną niewiedzę oceniającego, albo celowe działanie. Poniżej przedstawiamy kilka zrzutów ekranu z systemu:
(…)
W odniesieniu jeszcze do punktu 40 OPZ:
40) System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników

zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
Wykonawca przesłał Zamawiającemu taką odp:.
„System ISSec wyposażony jest we własny Moduł analizy podatności automatycznie sprawdzający wszystkie urządzenia oraz ich oprogramowanie zinwentaryzowane w systemie. Synchronizacje z bazami CVE odbywają się cyklicznie bez ingerencji użytkownika. Ponadto użytkownik z poziomu systemu może oznaczyć podatność jako rozwiązaną (zaakceptowaną). Po aktualizacji lub usunięciu oprogramowania wykryta wcześniej w systemie podatność zostanie automatycznie usunięta. Ponadto system ISSec umożliwia integracje z innymi skanerami podatności udostępniającymi API takimi jak np. Nessus 7 w powyżej przedstawionym zakresie. „
Zostało to również źle ocenione przez Zamawiającego, ponieważ nie znalazł „możliwości konfiguracji integracji przez API". Wykonawca oświadcza, że system iS Sec, którego jest producentem ma na tyle otwartą strukturę, że integruje się z każdym dostępnym na rynku skanerem podatności, który na taką integracje pozwala. W ramach wdrożenia systemu Wykonawca konfiguruje system tak, żeby był w pełni zintegrowany ze skanerem podatności, który posiada. Przedstawienie np. takiej integracji z trzema komercyjnymi skanerami podatności (innych producentów), wiązałoby się z zakupem tych licencji przez wykonawcę. Licencja dla wspomnianego w OPZ oprogramowania Nessus jest kosztem rzędu 100 tyś zł. rocznie. Wykonawca podejrzewa, że konkurencyjne firmy, specjalnie dla tego postępowania, nie zakupiły tej licencji i również nie przedstawiły wyników tej integracji. Wykonawca widział wyniki oceny wg. tej samej ankiety dla firmy, która została wyłoniona. Zamawiający w tej ankiecie dopuścił integrację (konfigurację integracji) z tymi skanerami pomimo tego, że trzeba było je wykonać z poziomu „powershell", czyli poza system Zamawianym. Czyli Zamawiający dla tej drugiej firmy dokonał oceny pozytywnej dla zewnętrznego mechanizmu konfigurującego omawiane integrację, a dla Odwołującego nie. Integracja poprzez API jest również zewnętrznym mechanizmem integrującym systemy, z tą różnicą, że jest to element systemu iS Sec, natomiast „powershell" jest elementem systemu Windows, który nie był przedmiotem zamówienia. Jak widać, system oferowany przez Odwołującego nie jest niezgodny z warunkami zamówienia w zakresie opisu przedmiotu zamówienia, To Zamawiający dokonał błędnej oceny dostarczonej próbki. Nie jest dla Zamawiającego żadnym usprawiedliwieniem to, że na spotkaniu w dniu 2 grudnia 2025 r. Odwołujący nie był w stanie zaprezentować powyższych wymagań, gdyż to Zamawiający nie informował o takiej potrzebie. Należy podkreślić, że Odwołujący jest producentem oferowanego systemu. Wyjaśnienia składane przez samego Odwołującego są oświadczeniami podmiotu najbardziej zaznajomionego z produktem, zarówno co do rozwiązań znanych, jak i tych utajnionych dla osób trzecich. Gdyby Zamawiający wyraził zgodę na dodatkowe spotkanie (co nie było zabronione), uzyskałby wszelkie niezbędne informacje pozwalające na uznanie, że oferowany system spełnia jego wymagania. Jak już wskazano, niezgodność systemu z opisem przedmiotu zamówienia zachodzi, gdy system nie posiada wymaganych funkcjonalności. Sytuacja taka nie zachodzi w niniejszym postępowaniu.
Zarzut nr 2
Zgodnie z art. 226 ust. 1 pkt 8) ustawy Pzp, Zamawiający odrzuca ofertę, jeżeli zawiera rażąco niską cenę lub koszt w stosunku do przedmiotu zamówienia.
Ustawa Prawo zamówień publicznych nie zawiera definicji rażąco niskiej ceny. Nie została ona również wskazana w Dyrektywach ani wypracowana przez Trybunał Sprawiedliwości Unii Europejskiej, jednak przez lata funkcjonowania regulacji badanie takiej ceny w kontekście weryfikacji ofert wykonawców, ukształtowane zostały kluczowe elementy tego pojęcia:
− o cenie rażąco niskiej można mówić wówczas, gdy oczywiste jest, że przy zachowaniu reguł rynkowych wykonanie umowy przez wykonawcę byłoby dla niego nieopłacalne (wyrok KIO z dnia 28 marca 2013 r., KIO 592/13),
− za ofertę z rażąco niską ceną można uznać ofertę z ceną niewiarygodną, nierealistyczną w porównaniu do cen rynkowych podobnych zamówień. Oznacza to cenę znacząco odbiegającą od cen przyjętych, wskazującą na fakt realizacji zamówienia poniżej kosztów wytworzenia usługi, dostawy, roboty budowlanej – cena dumpingowa (opinia prawna Urzędu Zamówień Publicznych),
− cena rażąco niska jest ceną nierealną, niepozwalającą na realizację zamówienia z należytą starannością, wskazującą na zamiar realizacji zamówienia poniżej kosztów własnych wykonawcy, nie pozwalającą na wygenerowanie przez niego zysku (wyrok KIO z dnia 17 czerwca 2019 r., KIO 992/19),
− cena rażąco niska jest to taka cena, która ewidentnie, w sposób obiektywnie i powszechnie widoczny jest nierealna (wyrok KIO z dnia 17 kwietnia 2023 r., KIO 835/23).
Odrzucając ofertę Odwołującego Zamawiający posłużył się argumentami domniemanymi, nie wskazując przy tym faktycznych wad złożonych wyjaśnień. Zamawiający kwestionuje wyjaśnienia dotyczące braku kosztów ukrytych, w tym związanych z zakupem akceleratora podnosząc, że „wedle jego wiedzy" takie koszty Odwołujący powinien ponieść. Odwołujący jest mocno zdziwiony, że Zamawiający wyciąga takie wnioski, nie znając architektury, systemu iS Sec. Sam zresztą w wezwaniu wskazał, że są to koszty „ewentualne". Nie znając technologii oraz nie znając zasad działania

metod uczenia maszynowego ML oraz sztucznej inteligencji AI. Wszystkie te wyliczenia i sugestie, są całkowicie bezpodstawne. Modele uczenia maszynowego stosowane w systemie ISSec to modele dotyczące wykrywania anomalii UEBA, które, uczą się na danych historycznych i douczają w trakcie, brak znajomości tych metod oraz zasady działania tych algorytmów skłania Zamawiającego do wyciągania tak absurdalnych wniosków. Oczywiście każda metoda ML obciąża CPU może obciążać GPU oraz nawet NPU. Ale metody ML stosowane w systemie iS Sec są tak dobrane, że technicznego punktu widzenia implementuje się je na Virtualnych maszynach które nie posiadają GPU i działają sprawnie. Model w trakcie uczenia się, douczania wymaga większej ilości zasobów natomiast sprawdzanie anomalii wykonywane jest paczkami, do maszyny z ML trafiają już tylko dan po preprocessingu i tylko wybrane cechy biorące udział w analizie. Zamawiający nie zna tych metod, nie zapytał jak działają, ale wyciągną wnioski że się nie da. Wykonawca natomiast wdrożył już kilkadziesiąt razy system iS Sec i nigdy klienci nie kupowali „akceleratorów" . Co do LLM, to również Zamawiający wykazał się całkowitym brakiem wiedzy na temat architektury realizacji itd. itp. Zazwyczaj modeli LLM nie implementuje się u odbiorców, tylko albo stawia się je na własnych zasobach, albo korzysta z rozwiązań chmurowych, albo po prostu korzysta się z API dostępnych modeli LLM. Takich jak Czat GPT, czy GEMINI, gdzie opłaty to pewnej ilości zapytań są zerowe bądź minimalne. Ciekawym argumentem Zamawiającego jest zakwestionowanie wyceny wsparcia technicznego w okresie dodatkowych 12 miesięcy. Wedle oceny Zamawiającego jest to niemożliwe do zrealizowania w cenie 10 000 zł. Jednocześnie Zamawiający nie znajduje podstaw do kwestionowania wyceny przyjętej przez TK-MED Sp. z o.o., która wynosi 1 000,00 zł (…).Odnosząc to do argumentacji Zamawiającego, który uważa, że 40 godzin w skali roku to zbyt mała ilość dla obsługi zamówienia, to nawet taka ilość godzin w odniesieniu do oferty TK-MED. Sp. z o.o. sugeruje godzinę pracy specjalisty na poziomie 25 zł, a więc poniżej płacy minimalnej. Ale tu już Zamawiający wątpliwości nie ma, co tylko potwierdza, że ocena Zamawiającego toczy się wedle podwójnych standardów faworyzujących jedną stronę. Odnosząc się jednak do argumentacji Zamawiającego, przenoszenie wynagrodzenia specjalisty, obliczonego w odniesieniu do prac konfiguracyjnych indywidualnie go angażujących, do wsparcia technicznego, które realizowane jest na zupełnie innych zasadach, w ramach ogólnego wsparcia klientów Odwołującego jest całkowicie chybione i ponownie jest działaniem pod z góry założoną tezę. Całość argumentacji Zamawiającego w przedmiocie rzekomo rażąco niskiej ceny w ogóle nie podważa realności wyceny systemu Odwołującego, a stanowi jedynie pustą polemikę. Odwołujący złożył obszerne wyjaśnienia ze wskazaniem wszystkich istotnych kosztów, które w pełni potwierdzają, że zaoferowana cena pozwala na wykonanie zamówienia zgodnie z wymaganiami Zamawiającego.

Zarzut nr 3

Zgodnie z art. 226 ust. 1 pkt 5) ustawy Pzp, Zamawiający odrzuca ofertę Wykonawcy, jeżeli jej treść jest niezgodna z warunkami zamówienia. Warunki zamówienia należy rozumieć zgodnie z definicją wyrażoną w art. 7 pkt 29 Pzp, która stanowi, że poprzez warunki zamówienia należy rozumieć warunki, które dotyczą zamówienia lub postępowania o udzielenie zamówienia, wynikające w szczególności z opisu przedmiotu zamówienia, wymagań związanych z realizacją zamówienia, kryteriów oceny ofert, wymagań proceduralnych lub projektowanych postanowień umowy w sprawie zamówienia publicznego. Jak już wskazano we wcześniejszej części odwołania, Opis przedmiotu zamówienia jednoznacznie wskazuje, że System musi spełniać następujące wymagania:

− Proces normalizacji musi wspierać następujące typy składni: CEF, LEEF, URI, SYSLOG (zgodny z RFC 3164) automatycznie tworzyć na ich podstawie pola i ich wartości zgodne z zasadami określonymi przez te składnie. Parsowanie powyższych składni nie może być realizowane za pomocą wyrażeń regularnych.

− System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX.

Jak wykazał Odwołujący, system oferowany przez TK-MED Sp. z o.o. nie posiada powyższych funkcjonalności w zakresie składni URI, co sam stwierdził Zamawiający podczas dokonanej oceny próbki. Jednoznacznie potwierdza to, że oferta TK-MED Sp. z o.o. jest niezgodna z warunkami zamówienia w zakresie, w jakim warunki te wynikają z opisu przedmiotu zamówienia. Tym samym, oferta ta powinna zostać odrzucona, a nie wybrana jako najkorzystniejsza jak uczynił to Zamawiający. Działanie Zamawiającego narusza również art. 16 pkt 1 i 2 ustawy Pzp, zgodnie z którymi postępowanie przeprowadza się z zachowaniem uczciwej konkurencji i równego traktowania wykonawców jak również w sposób przejrzysty.

Zarzut nr 4:

Zgodnie z art. 239 ust. 1 i 2 ustawy Pzp, Zamawiający wybiera najkorzystniejszą ofertę na podstawie kryteriów oceny ofert określonych w dokumentach zamówienia. Najkorzystniejsza oferta to oferta przedstawiająca najkorzystniejszy stosunek jakości do ceny lub kosztu lub oferta z najniższą ceną lub kosztem. Potwierdzenie zarzutu 3 prowadzi wprost to uznania, że wybór oferty obarczony jest wadą. Oferta podlegająca odrzuceniu nie może być ofertą wybraną.

Zarzut nr 5 i 6 (zarzut ewentualny):
Zgodnie z art. 255 pkt 6) Pzp Zamawiający unieważnia postępowanie o udzielenie zamówienia publicznego, jeżeli postępowanie obarczone jest niemożliwą do usunięcia wadą uniemożliwiającą zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego. Zamawiający ma obowiązek unieważnienia postępowania o udzielenie zamówienia ze względu na jego wadę, o ile spełnia ona dwa kryteria. Musi to być wada niemożliwa do usunięcia po jej stwierdzeniu ze względu na stan zaawansowania postępowania. Ponadto chodzi o nieprawidłowości rzutujące bezpośrednio na zawarcie niepodlegającej unieważnieniu umowy w sprawie zamówienia publicznego. Celem postępowania jest bowiem zawarcie wyłącznie w pełni skutecznej umowy w sprawie zamówienia publicznego. Na przeszkodzie stają zatem wyłącznie nieusuwalne wady proceduralne (nie podlegające konwalidacji), obciążające postępowanie w sposób nieodwracalny. Mogą to być zarówno nieprawidłowe działania, jak i zaniechania zamawiającego.
W ocenie Odwołującego w postępowaniu Zamawiający dokonał tak dalece nieprawidłowego opisu przedmiotu zamówienia w zakresie procedury oceny próbki systemu, że niemożliwe jest na obecnym etapie postepowania:
− zagwarantowanierównego traktowania wykonawców i uczciwej konkurencji,
− dokonanie obiektywnej oceny oferowanych systemów.
Powyższe narusza art. 99 ust. 1 i 4 ustawy Pzp.
Zgodnie z art. 457 ust. 1 pkt 1) ustawy Pzp, Umowa podlega unieważnieniu, jeżeli zamawiający z naruszeniem ustawy udzielił zamówienia, zawarł umowę ramową lub ustanowił dynamiczny system zakupów bez uprzedniego zamieszczenia w Biuletynie Zamówień Publicznych albo przekazania Urzędowi Publikacji Unii Europejskiej ogłoszenia wszczynającego postępowanie lub bez wymaganego ogłoszenia zmieniającego ogłoszenie wszczynające postępowanie, jeżeli zmiany miały znaczenie dla sporządzenia wniosków o dopuszczenie do udziału w postępowaniu albo ofert. Zgodnie z wyrokiem KIO 310/23, nie można przyjąć, że „z art. 457 ust. 1 pkt 1 Prawa zamówień publicznych wynika wyłącznie przesłanka unieważnienia umowy, związana z nieprawidłowościami w obowiązkowych ogłoszeniach w publikatorach. Każde naruszenie związane z ogłoszeniami jest równocześnie "naruszeniem ustawy". Trzeba zatem przyjąć, że ustawodawca przewidział dwie podstawy unieważnienia, do których odwołuje się w art. 457 ust. 1 pkt Prawa zamówień publicznych, tj: "do zawarcia umowy z naruszeniem Pzp oraz do zaniechania obowiązków ogłoszeniowych" (tak: Prawo zamówień komentarz, red. Hubert Nowak i Marek Winiarz, Urząd Zamówień Publicznych, Warszawa 2021). Rzeczywiście przepis sformułowany jest mało przejrzyście, ale trudno byłoby zaakceptować, dlaczego ustawodawca, jako prowadzącą do nieważności umowy, miałby przyjąć jedynie przesłankę związaną z ogłoszeniami, mającymi znaczenie dla sporządzenia ofert, a pominął inne naruszenia przepisów, które takie znaczenia również mają. Dlatego zasadnym jest przyjęcie, że intencją ustawodawcy było wprowadzenie przesłanki nieważności umowy zawartej z naruszeniem przepisów Prawa zamówień publicznych, jednak nie każdym, tylko kwalifikowanym - takim, które miało znaczenie dla przygotowania ofert, a więc wpłynęło na wynik postępowania. Generalnie rzecz biorąc przesłanki unieważnienia postępowania mają charakter wysoce sankcyjny i powinny być interpretowane możliwie wąsko, jednak jakakolwiek interpretacja musi uwzględniać sens i cel przepisu. Dlatego ostatecznie, biorąc pod uwagę powyższe rozważania, Izba doszła do wniosku, że udzielenie zamówienia z naruszeniem przepisów ustawy, tego rodzaju, że miało wpływ na sporządzenie ofert i wynik postępowania, mieści się w normie opisanej w art. 457 ust. 1 pkt 1 Prawa zamówień publicznych.” Również w wyroku KIO 169/22 Izba uznała, że „konstrukcja przepisu odsyła wprost do art. 457 ust. 1 ustawy Pzp, w którym wymienione są wszystkie przypadki naruszenia Pzp powodujące konieczność unieważnienia umowy. Odesłania nie można jednak ograniczać wyłącznie do przywołanego przepisu, który zawiera zamknięty i bardzo ograniczony katalog sytuacji powodujących unieważnienie umowy. Taka interpretacja skutkowałaby tym, iż wystąpienie innych wad w postępowaniu nie mogłoby być powodem jego unieważnienia. Taka wykładnia prowadziłaby do błędnego zdaniem Izby wniosku, że nawet wystąpienie wady w sposób oczywisty wypaczającej wynik postępowania nie daje zamawiającemu prawa do unieważnienia postępowania, podczas gdy zawarcie umowy będzie rodzić skutki w postaci dochodzenia jej nieważności lub unieważnienia przez innych wykonawców na podstawie odrębnych przepisów, czego w przypadku wad innych niż określone art. 457 ust. 1 pkt 1 Pzp nie zabrania. Izba zwraca uwagę, że w przepisach ustawy Pzp istnieje możliwość uznania umowy za nieważną na podstawie art. 457 ust. 5 ustawy Pzp który stanowi, że przepis ust. 1 nie wyłącza możliwości żądania unieważnienia umowy na podstawie art. 705 ustawy z dnia 23 kwietnia 1964 r. - Kodeks cywilny. Dyspozycja art. 705 k.c. znajdzie zastosowanie do umów w sprawie zamówień publicznych zawartych w wyniku jakiegokolwiek postępowania otwartego (poprzedzonego ogłoszeniem) prowadzonego w oparciu o przepisy Pzp. Możliwość żądania unieważnienia umowy w sprawie zamówienia publicznego w oparciu o art. 705 k.c. jest niezależna od podstaw i ograniczeń unieważnienia na podstawie przepisów Pzp.”
Powyższe poglądy Izby zasługują w pełni na uwzględnienie. Inny wniosek prowadziłby do uznania, że po terminie składania ofert Zamawiający nie ma prawa unieważnić postępowania w związku z wadami proceduralnymi, a więc musi udzielić zamówienia Wykonawcy wybranemu w takim wadliwym postępowaniu, chyba że zajdą inne przesłanki unieważnienia.

Nie budzi wątpliwości, że za wadę postępowania uzasadniającą jego unieważnienie może być uznana wada wynikająca z opisu przedmiotu zamówienia. W orzecznictwie Izby wykształcił się pogląd, że niejasność lub nieprecyzyjność opisu przedmiotu zamówienia może stanowić podstawę unieważnienia postępowania. Pogląd ten został wyrażony m.in. w wyrokach KIO: z 25 września 2017 r. (KIO 1869/17), z 4 sierpnia 2017 r. (KIO 1507/17), z 11 czerwca 2021 r. (KIO 1343/21) oraz z 18 lipca 2022 r. (KIO 1623/22). Przy czym niejednoznaczność opisu musi być na tyle znacząca, że porównanie złożonych ofert nie jest możliwe (zob. wyroki Izby z 24 września 2019 r., KIO 1747/19, oraz z 12 listopada 2019 r., KIO 2176/19). O braku jednoznaczności opisu przedmiotu zamówienia nie można natomiast mówić w sytuacji, gdy zamawiający konstruuje opis, który nie odzwierciedla jego rzeczywistych potrzeb (zob. wyrok KIO z 12 sierpnia 2021 r., KIO 2309/21). Jak wykazano już w odwołaniu, Zamawiający dokonał takiego opisu przedmiotu zamówienia, który:
1)jednocześnie wymusza istnienie określnych funkcjonalności systemu („system musi posiadać") i dopuszcza sytuację, w której jedna lub więcej tych funkcjonalności jednak nie jest spełniona nie powodując negatywnej oceny oferowanego produktu, a ocena w tym zakresie ma charakter następczy – po złożeniu ofert;
2)przyznaje Zamawiającemu prawo oceny w oparciu o subiektywne odczucia w zakresie, którego nie opisał, a który mógł określić przed terminem składania ofert.
Należy zauważyć, że „Intuicyjność" ma w ocenie próbki wagę 25 %. Uwzględniając przy tym zapis, że każdy punkt musi osiągnąć minimum 90 %, jest to prosty sposób eliminowania oprogramowania bez logicznego uzasadnienia i w sposób nieproporcjonalny, co zresztą potwierdza badanie Zamawiającego.
Zamawiający jako rozwiązanie nieintuicyjne wskazuje m.in.:
− Wymagane jest przepisanie numeru zdarzenia który ma łącznie 32 cyfry w formacie heksadecymalnym połączone w pięć grup. Nie ma możliwości wyszukania po części numeru. Sama nazwa funkcji nie wskazuje na to że służy do grupowania zdarzeń;
− Opis zawiera tylko i wyłącznie ręczne przypisywanie zdarzeń, funkcja automatycznego przypisywania zdarzeń nie została odnaleziona;
− Wszystkie nazwy po angielsku, brakuje opisów i wyjaśnienia co dana funkcja robi.
Istnieje możliwość wyszukiwania po nazwie.
Każdy z tych elementów mógł być opisany jako oczekiwany w ramach funkcjonalności, ale Zamawiający tego zaniechał, a teraz dokonuje w oparciu o te elementy oceny warunkujące to czy oferta podlega lub nie podlega odrzuceniu.
Praktyka taka przeczy podstawowym zasadom zamówień publicznych wyrażonym w art. 16 ustawy Pzp.
Mając na uwadze powyższe, wnoszę jak na wstępie.
(…)
V.Wpływ na wynik postępowania
Zgodnie z art. 554 ust. 1 Pzp Izba uwzględnia odwołanie, jeżeli stwierdzi naruszenie przepisów ustawy, które miało wpływ lub może miéć istotny wpływ na wynik postępowania o udzielenie zamówienia. Przedstawiony w odwołaniu stan faktyczny jak i dokonana analiza prawna potwierdzają, że w postępowaniu Zamawiający naruszył przepisy w taki sposób, że zaburzył wynik postępowania. Udzielenie zamówienia w takich okolicznościach, będzie działaniem sprzecznym z ustawą.

Do postępowania odwoławczego po stronie Zamawiającego przystąpienie w piśmie z dnia 30.12.2025 r. zgłosił wykonawca TK-MED Sp. z o.o. z/s w Chorzowie (Uczestnik po stronie Zamawiającego) wnoszą o oddalenie odwołania.
W uzasadnieniu stanowiska podał: (…)
I.Interes przystępującego
Przystępujący po stronie Zamawiającego – spółka TK-MED Sp. z o.o. złożyła ofertę w postępowaniu o udzieleniu zamówienia publicznego prowadzonego pn.: „Dostawa i wdrożenie systemu bezpieczeństwa SIEM/SOAR w ramach projektu grantowego >>Cyberbezpieczny Samorząd<<" przez Powiat Żyrardowski. Zgodnie z informacją o wyborze najkorzystniejszej oferty z dnia 17 grudnia 2025 roku, oferta złożona przez Przystępującego była jedyną ofertą niepodlegającą odrzuceniu. Co więcej, w toku postępowania ofertę złożyły zaledwie dwa podmioty, a drugim wykonawcą jest Odwołujący - spółka InfoSoftware Polska Sp. z o.o. Oferta złożona przez Odwołującego została odrzucona przez Zamawiającego na zasadzie art. 226 ust. 1 pkt 5 pzp oraz art. 226 ust. 1 pkt 8 pzp. Za najkorzystniejszą ofertę złożoną w postępowaniu została wybrana ta, złożona przez Przystępującego.
Przystępujący posiada zatem oczywisty interes prawny w uzyskaniu rozstrzygnięcia na korzyść Zamawiającego i jest zainteresowany utrzymaniem w mocy wyżej wymienionych czynności. Ewentualne uwzględnienie odwołania przez KIO miałoby bezpośredni i negatywny wpływ na sytuację Przystępującego, albowiem uniemożliwiałoby mu to realizację przedmiotu zamówienia publicznego, a tym samym uzyskanie z tego tytułu wynagrodzenia.
II.Stanowisko Przystępującego
W ocenie Przystępującego zarzuty sformułowane przez Odwołującego pozostają nietrafione, albowiem wszystkie

czynności podjęte przez Zamawiającego odpowiadają wymogom stawianym przez przepisy pzp. Przytaczana przez Odwołującego argumentacja stanowi w istocie jedynie polemikę z prawidłowymi ustaleniami Zamawiającego podjętymi wskutek weryfikacji obu oferowanych systemów informatycznych. W konsekwencji, odwołanie jako niezasadne nie zasługuje na uwzględnienie i winno zostać oddalone.

Odnosząc się pokrótce do kolejnych zarzutów podnoszonych przez Odwołującego wskazać w pierwszej kolejności należy, iż oferta Odwołującego została zasadnie odrzucona przez Zamawiającego w oparciu o art. 226 ust. 1 pkt 5 pzp, albowiem jej treść nie była zgodna z warunkami zamówienia. Odwołujący w piśmie procesowym szeroko odnosi się do poszczególnych wad stwierdzonych przez Zamawiającego podczas dokonywania oceny dostarczonej próbki oprogramowania wywodząc, iż ocena dokonana przez Zamawiającego była błędna. Odnosząc się do nich tych uwag zbiorczo, zaakcentowania wymaga przede wszystkim pkt 144 zd. 3 Załącznika nr 8 do SWZ „*W przypadku, gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona*." Oznacza to, że Zamawiający jasno sformułował w SWZ postanowienia, iż nieodnalezienie określonej funkcjonalności będzie skutkowało odrzuceniem oferty. Aby przeciwdziałać przypadkowemu przeoczeniu danej funkcjonalności Zamawiający przewidział specjalną procedurą opisaną szczegółowo w pkt 145 lit. g Załącznika nr 8 do SWZ, zgodnie z którym „Wykonawca w okresie 3 dni od otrzymania oceny strony Zamawiającego (ppkt. f) ma możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego odniesie się on do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. Jeśli w wyznaczonym terminie Wykonawca nie zorganizuje spotkania i/lub nie przedstawi odpowiedzi na ocenę Zamawiającego zostanie uznane, że oferowane rozwiązanie nie spełnia wymagań OPZ".

Oznacza to z jednej strony, iż Odwołujący miał prawo do zajęcia stanowiska i odniesienia się do uwag Zamawiającego jeszcze na etapie oceny próbek przedmiotu zamówienia. Z drugiej strony oznacza to jednak, iż ciężar dowodowy w takim przypadku (pkt 145 lit. g) został de facto przerzucony na Odwołującego, albowiem to on był zobowiązany do wykazania, iż zaoferowany przez niego system IT spełniał wymagania wbrew pierwotnej ocenie Zamawiającego. Procedurę tę należy zatem uznać za swoiste wezwanie do udzielenia wyjaśnień. Z przytoczonego przez Odwołującego stanu faktycznego wynika, iż do organizacji spotkania w trybie zdalnym de facto doszło, jednak złożone przez Odwołującego wyjaśnienia okazały się niewystarczające. Nie może dziwić, że Zamawiający oczekiwał prezentacji każdego z kwestionowanych wymagań, wobec niepopartych twierdzeń oferenta. Zgodnie z przytoczonym pkt 145 lit. g Załącznika nr 8 do SWZ, to właśnie to spotkanie w formie zdalnej miało służyć rozwianiu jakichkolwiek wątpliwości Zamawiającego. Z wniesionego odwołania wynika, że Odwołujący nie był jednak przygotowany na taką okoliczność i nie przeprowadził takiej prezentacji, a więc de facto nie przedstawił odpowiedzi na ocenę Zamawiającego. Dość wskazać, że procedura opisana w Załączniku nr 8 do SWZ nie przewidywała możliwości organizacji ponownego spotkania w jakimkolwiek trybie, toteż wyrażenie zgody na takowe przez Zamawiającego stanowiłoby naruszenie zasad postępowania i faworyzację jednego z wykonawców. Tym samym, Zamawiający słusznie (w oparciu o pkt 144 zd. 3 oraz pkt 145 lit. g. Załącznika nr 8 do SWZ) uznał, że oferowane rozwiązanie nie spełnia wymagań OPZ.

Gdyby Odwołujący równie szeroko, co w odwołaniu odniósł się do poszczególnych wad stwierdzonych przez Zamawiającego we właściwym czasie tj. podczas spotkania w trybie

5 zdalnym, Zamawiający mógłby dokonać weryfikacji własnych ustaleń. Wobec niewykorzystania przedmiotowej szansy, czynione obecnie wyjaśnienia uznać należy za co najmniej spóźnione. Rolą KIO w tego typu sprawach nie jest ponowna ocena całego systemu IT oferowanego przez Odwołującego, a to czy Zamawiający dokonując odrzucenia jego oferty naruszył przepisy ustawy lub postanowienia SWZ. Tymczasem, z przedstawionego stanu faktycznego jasno wynika, iż działania Zamawiającego znajdowały pełne oparcie w precyzyjnie opisanej w SWZ procedurze.

Mając na uwadze powyższe, stawiany przez Odwołującego zarzut naruszenia przez Zamawiającego art. 226 ust. 1 pkt 5 pzp jawi się jako zupełnie bezzasadny.

Po drugie, należy przyznać rację Zamawiającemu, który uznał, iż oferta Odwołującego zawiera rażąco niską cenę w stosunku do przedmiotu zamówienia. Odwołujący stawiając zarzut naruszenia art. 226 ust. 1 pkt 8 pzp podniósł, iż Zamawiający nie zaakceptował wyjaśnień udzielonych przez Odwołującego. Rzecz jednak w tym, że uzasadniając przedmiotowy zarzut,

Odwołujący ograniczył się jedynie do skierowania wobec Zamawiającego słów krytyki imputując mu brak znajomości technologii czy zasad działania metod uczenia maszynowego. Tymczasem, w przypadku rozpoznania zarzutu rażąco niskiej ceny, na etapie postępowania odwoławczego ciężar dowodu rozkłada się analogicznie do tego w postępowaniu o udzielenie zamówienia. Oznacza to, że stosownie do art. 537 pzp ciężar dowodu, że oferta nie zawiera rażąco niskiej ceny, bądź też że cena nie budzi wątpliwości, spoczywa na wykonawcy który ją złożył. Zgodnie z utrwalonym orzecznictwem Krajowej Izby Odwoławczej, treść art. 537 pzp nie uprawnia Odwołującego do poprzestania na samych twierdzeniach i przerzucenia na uczestnika postępowania lub Zamawiającego ciężar dowodu (por. wyrok KIO z dnia 26

kwietnia 2022 r. o sygn. akt KIO 719/22 oraz wyrok KIO z dnia 21 stycznia 2019 r. o sygn. akt KIO 2617/18).
Mając na uwadze powyższe wskazać należy, iż w ocenie Przystępującego, Odwołujący nie sprostał ciężarowi dowodowemu i nie wykazał, że oferta nie zawiera rażąco niskiej ceny. W toku postępowania, Zamawiający słusznie powziął wątpliwości co do rynkowego charakteru ceny zawartej w ofercie Odwołującego i wezwał go do złożenia stosownych wyjaśnień. Dość wskazać w tym miejscu, że cena zaoferowana przez Odwołującego była ponad dwukrotnie niższa od tej przedstawionej przez Przystępującego, jak i ponad dwukrotnie niższa od kwoty jaką Zamawiający zamierzał przeznaczyć na sfinansowanie zamówienia. Zamawiający słusznie zakwestionował wyjaśnienia Odwołującego i uznał zaoferowaną cenę za rażąco niską. Przedstawiona przez Odwołującego argumentacja w złożonym odwołaniu nie może doprowadzić do zmiany dokonanej przez Zamawiającego ceny.
Mając na uwadze powyższe, stawiany przez Odwołującego zarzut naruszenia przez Zamawiającego art. 226 ust. 1 pkt 8 pzp jawi się jako zupełnie bezzasadny.
Po trzecie, nie sposób zgodzić się z zarzutem nr 3 sformułowanym przez Odwołującego, a dotyczącym rzekomej niezgodności z warunkami zamówienia oferty Przystępującego. Zamawiający precyzyjnie określił w jakich sytuacjach wymagania wskazane w Załączniku nr 8 do SWZ zostaną uznane za spełnione. Jedynie na marginesie wskazać należy, że Odwołujący sam dokonał ich przytoczenia na stronie siódmej odwołania. Zgodnie z pkt 145 lit f. „Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%." Z kolei, zgodnie z pkt 145 lit. e, ocena każdego z wymagań miała nastąpić z uwzględnieniem kryterium intuicyjności (25%) oraz zgodności (75%). Wskazać należy, iż w formularzu oceny systemu oferowanego przez Przystępującego, kwestionowane przez Oferującego wymaganie zostało ocenione przez Zamawiającego w wierszu (l.p.) nr 2 odnoszącym się do pkt 11 w OPZ. Z powodu braku wspierania składni URI Zamawiający ocenił zgodność na poziomie 67% (na 75% możliwych), jednak ocenę intuicyjności na poziomie 25%, co sumarycznie oznaczało ocenę 92%. Zważywszy zatem, że w myśl przytoczonego pkt 145 lit. f. Załącznika nr 8 do SWZ, wymaganie uznaje się za spełnione w przypadku oceny na poziomie co najmniej 75%, nie może ulegać wątpliwości, iż oferta Przystępującego jest zgodna z warunkami zamówienia. W konsekwencji, stawiany przez Odwołującego zarzut naruszenia przez Zamawiającego art. 226 ust. 1 pkt 5 pzp pozostaje niezasadny.
Odnosząc się do zarzutu czwartego sformułowanego przez Odwołującego godzi się zauważyć, że ma on charakter wtórny, a ocena jego zasadności wynika wprost z oceny uprzednio omówionych zarzutów. Biorąc z kolei pod uwagę, iż te pozostają nietrafione, również i zarzut nr 4 nie zasługuje na uwzględnienie.
Przechodząc do sformułowanych przez Odwołującego zarzutów ewentualnych – wynika z nich, iż Odwołujący upatruje wadliwości postępowania uzasadniającej jego unieważnienie w dwóch argumentach tj. niejasności opisu zamówienia oraz przyznania oceny w oparciu o subiektywne odczucia. Pierwszy z powyższych stanowi w istocie powielenie zarzutu nr 3 dotyczącego sposobu oceny wymagań stawianych w OPZ. W ocenie Przystępującego, zasady oceny zostały precyzyjnie określone w Załączniku nr 8 do SWZ, a Przystępujący odniósł się do nich już we wcześniejszym fragmencie niniejszego pisma. Z powyższych względów powielanie przedmiotowej argumentacji w tym miejscu jawi się jako bezcelowe.
Drugi argument podnoszony przez Odwołującego odnosi się w istocie do zakwestionowania przesłanki „intuicyjności" do oceny oferowanego systemu IT. Tymczasem „intuicyjność" jako kryterium jakościowe jest powszechnie wykorzystywane w praktyce i aprobowane w orzecznictwie, zwłaszcza gdy przedmiotem zamówienia są właśnie systemy IT. Nie sposób zgodzić się ze stanowiskiem Odwołującego, iż kryterium to dawało Zamawiającemu pełną swobodę „w eliminowaniu oprogramowania bez logicznego uzasadnienia i w sposób
8 nieproporcjonalny". Przeciwnie, należy zauważyć, że Zamawiający przyznał kryterium intuicyjności 25% wagi oceny. Jednocześnie, jak przytoczono już wcześniej, wymaganie uznawało się za spełnione w przypadku oceny na poziomie co najmniej 75%. Oznacza to, że jeżeli dana funkcjonalność systemu była w pełni zgodna z oczekiwaniami Zamawiającego, to nawet w przypadku całkowitego braku intuicyjności i dokonania jej oceny na poziomie 0%, wymaganie należy uznać za spełnione. Tym samym, kryterium intuicyjności nie może samodzielnie prowadzić do subiektywnego eliminowania ofert wykonawców.
Co więcej, zgodnie z pkt 145 lit. g wykonawca miał prawo w terminie trzech dni od dnia otrzymania wyników oceny do wyznaczenia spotkania w formie zdalnej, celem odniesienia się do wyników oceny zgodności i intuicyjności systemu. Oznacza to, że Zamawiający przyznał wykonawcom prawo de facto złożenia wyjaśnień już po przeprowadzeniu oceny oferowanych przez nich systemów informatycznych. Choć Przystępujący nie ma wiedzy o przebiegu przedmiotowego spotkania, nie sposób podzielić argumentacji Odwołującego zawartej na 48 stronie in fine odwołania. W ocenie Przystępującego, wszystkie przytoczone przez Odwołującego rozwiązania zostały zasadnie uznane przez Zamawiającego za nieintuicyjne. (…)

Zamawiający w odpowiedzi na odwołanie (pismo z dnia 6.02.2026 r.) wniósł o oddalenie odwołania w całości. W uzasadnieniu stanowiska wskazał: (…)

I. Zarzut dotyczący naruszenia art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) - 3) ustawy (…) – (…).

Każde zamówienie publiczne ma zamierzony cel, którego osiągnięcie jest możliwe w wyniku postępowania. Cel ten stoi ponad interesem wykonawców ubiegających się o zamówienie. Celem tym jest zaspokojenie konkretnych, obiektywnie uzasadnionych potrzeb zamawiającego poprzez efektywne wydatkowanie środków.

Prawo zamawiającego do określania parametrów technicznych, funkcjonalnych i jakościowych nie jest nieograniczone, ale granice te wyznaczają uzasadnione potrzeby. Jak wskazuje doktryna, zamawiający ma prawo opisać przedmiot zamówienia w sposób, który może ograniczać krąg potencjalnych wykonawców, pod warunkiem, że wymagania te są proporcjonalne do celu zamówienia i wynikają z obiektywnych potrzeb.

Zamawiający nie ma obowiązku obniżania swoich wymagań do poziomu „przeciętnej oferty rynkowej" ani dostosowywania opisu przedmiotu zamówienia do możliwości „przeciętnego wykonawcy". Jeśli zamawiający wymaga specyficznej funkcjonalności, to fakt, że dany system realizuje to w inny sposób, nie czyni oferty zgodną.

Zakup systemu bezpieczeństwa (SIEM/SOAR) jest działaniem na rzecz ochrony interesu publicznego. W tym kontekście specyficzne, precyzyjne wymagania techniczne są uzasadnione koniecznością zapewnienia poziomu bezpieczeństwa i ergonomii pracy osób, które nabywany system będą obsługiwać w celu zapewnienia zbiorowej ochrony cyfrowej.

Opis przedmiotu zamówienia prezentujący konkretne wymagania funkcjonalne jest oczekiwaniem Zamawiającego co do konkretnego rezultatu działania systemu. Argumentacja opierająca się na twierdzeniu, że produkt (tu: system bezpieczeństwa) jest wystarczająco dobry lub realizuje cel w inny sposób podlega odrzuceniu *a limine*.

Postępowanie o udzielenie zamówienia nie jest też polem do wzajemnych ustępstw (poza trybami negocjacyjnymi), lecz procedurą sformalizowaną, w której oferta musi stanowić lustrzane odbicie wymagań zamawiającego. Jeśli jest inaczej, mamy do czynienia z niezgodnością treści oferty z warunkami zamówienia.

Zanim Zamawiający odniesie się do poszczególnych punktów składających się na ww. zarzut, należy we wstępie przybliżyć również rolę próbki. Otóż w niniejszym Postępowaniu próbka w formie dostępu demonstracyjnego pełniła funkcję przede wszystkim dowodową. Zgodnie z systematyką Ustawy, próbka jest przedmiotowym środkiem dowodowym. Służy potwierdzeniu, że oferowany system spełnia wymagania określone przez zamawiającego. Zatem próbka ma udowodnić, że system działa tak, jak opisano w opisie przedmiotu zamówienia. Nie jest to jedynie ilustracja możliwości wykonawcy i jego wizji systemu, lecz dowód. Ponadto obok funkcji dowodowej, próbka stanowi również element oferty. Pokazuje ona konkretne rozwiązania, które wykonawca oferuje i wykazuje spełnienie wymagań. Jeśli próbka nie zawiera pewnych funkcji wymaganych względem niej i później całego systemu, przyjmuje się, że oferowany system ich nie posiada. Próbkę należy zatem traktować jako wycinek możliwości produktu wykonawcy w momencie składania ofert. Zamawiający bada ten wycinek systemu, aby ocenić całość. Samo badanie odbywa się z kolei o przygotowane scenariusze testowe. Wykonawca, chcąc uzyskać zamówienie, musi przygotować próbkę w taki sposób, aby Zamawiający mógł bez trudu zweryfikować wymagane cechy. Próbka powinna być przyjąć takie parametry, aby umożliwić weryfikację bez konieczności posiadania wiedzy eksperckiej o wewnętrznej architekturze specyficznego produktu wykonawcy. Z kolei na Zamawiającym ciąży zakaz domniemania posiadania funkcji przez oferowany system: jeśli funkcja nie została zademonstrowana albo obligatoryjna instrukcja nie wykazuje jej istnienia, uznaje się ją za nieistniejącą w momencie jej badania.

W dalszej części Zamawiający odniesie się do każdego punktu składającego się na ww. zarzut, zgodnie z systematyką odwołania i przy zachowaniu przyjętej kolejności.

Punkt 1 opisu przedmiotu zamówienia

Wbrew twierdzeniom Odwołującego (str. 11 odwołania), jakoby system wykorzystywał jedynie silnik bazy danych Elasticsearch, materiał dowodowy ujawnia wykorzystanie parametru o nazwie Elastic_Agent (nagranie „Reguły korelacyjne IS Sec.mkv", czas 04:30).

9.Powyższy zrzut ekranu z interfejsu właściwego dla nowej reguły korelacyjnej prezentuje widoczną na liście filtrów/warunków „elastic_agent.id.keyword". Obecność tego konkretnego parametru dowodzi, że system posiada zainstalowanego agenta Elastic Agent, będącego integralną częścią platformy Elastic Security.

10.Zgodnie z dokumentacją producenta1, Elastic Agent nie jest bazą danych. Jest to dedykowane oprogramowanie służące m.in. do aktywnej ochrony stacji końcowych (Security) i stanowi integralny element rozwiązania Elastic Security, wymienionego w pkt. 1 opisu przedmiotu zamówienia jako niedozwolony. Parametr Elastic Agent stanowi element oprogramowania systemu bezpieczeństwa Elastic Security. Elastic A w graficzny interfejs (GUI) do tworzenia reguł

normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o konkretne składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX. Zamawiający nie wymagał jedynie "możliwości obsługi" tych formatów, ale wymag konkretnego narzędzia w interfejsie graficznym dedykowanego tym formatom.

12.W toku badania oferty Odwołującego (testu próbki), Zamawiający stwierdził brak funkcjonalności parsowania dla formatów CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX z poziomu graficznego interfejsu. Odwołujący w piśn przedstawił zrzuty ekranu jako materiał dowodowy, z których nie wynika wniosek przeciwny. Otóż na załączonych zrzutach ekranu widnieje funkcja „Dodaj procesor", a niżej widoczna jest lista rozwijana „Typ". Zawiera ona opcje takie jak: Konwersja na bajty, Konwersja okręgu, Identyfikator społeczności, Konwersja typu danych, CSV, Data, Nazwa indeksu z datą, Rozszerzanie notacji kropkowej, Usuwanie dokumentu, Komunikat o błędzie, Skrót zawartości dokumentu, Geosiatka, Dodawanie danych geograficznych, Wyrażenie regularne [Grok], Wyrażenie regularne [Gsub], Usuwanie znaczników HTML, Łączenie ciągów. Na kolejnym zrzucie widoczne są dodatkowe opcje: Konwersja URI, Tworzenie obiektu JSON. Na żadnym z dostarczonych zrzutów ekranu oferowanego systemu nie widnieją dedykowane opcje: CEF, LEEF, XML czy SYSLOG, abstrahując od ewentualnego sposobu ich działania, którego w oparciu o zrzuty ekranu nie sposób zweryfikować. Zamiast tego Odwołujący oferuje ogólny procesor "Wyrażenie regularne [Grok]", co w ocenie Zamawiającego stanowi próbę zmiany sposobu obsługi systemu w stosunku do wymagań.

13.Dodatkowo Zamawiający podnosi, że Odwołujący w przesłanych dokumentach nie definiuje jednoznacznie, czym w istocie jest oferowana przez niego składnia „GROK". Brak tej definicji w materiałach Odwołującego narusza wymóg dostarczenia odpowiedniej dokumentacji – por. pkt 144 opisu przedmiotu zamówienia. To właśnie weryfikacja oferowanego systemu w postaci jego próbki i dostarczonej dokumentacji była podstawą kontroli spełnienia wymogów. Podkreślenia wymaga, że nie tylko niezgodność systemu z wymaganiami, ale też niezgodność dokumentacji z opisem przedmiotu zamówienia lub sam brak dokumentacji, stanowiły podstawę odrzucenia oferty. Dokumentacja dostarczona przez Odwołującego była na tyle niekompletna i pozbawiona warstwy merytorycznej, że Zamawiający zmuszony był wyszukiwać informacji w zewnętrznych, ogólnie dostępnych źródłach, co z pewnością stanowi argument obalający twierdzenie Odwołującego o braku dobrej woli Zamawiającego do zapoznania się z systemem. Dokumentacja tej treści skutecznie utrudniała zapoznanie się z funkcjami systemu.

14.W tym miejscu Zamawiający uznaje za zasadne przedstawienie różnicy pomiędzy składnią GROK a wymienionymi formatami ustrukturyzowanymi. Składnia GROK narzędziem do obsługi danych nieustrukturyzowanych i służy do analizy tekstu linijka po linijce (liniowo). Potwierdza to dokumentacja firmy Elastic (twórcy standardu GROK) - Logstash Grok Filter Plugin . W przeciwieństwie do dedykowanych parserów XML/JSON, GROK nie interpretuje hierarchicznej struktur danych (drzewa), co sprawia, że jego użycie do tych formatów jest niezgodne z przeznaczeniem. Format XML to również format hierarchiczny, drzewiasty: „XML documents form a tree structure that starts at "the root" and branches to "the leaves" (tłumaczenie: Dokumenty XML tworzą strukturę drzewa, która zaczyna się od „korzenia" i rozgałęzia się do „liści".) . Oznacza to tyle, że organizacja danych to relacja nadrzędny – podrzędny. Dostęp do konkretnej informacji wymaga przejścia ścieżki od „korzenia" przez „gałęzie" do „liścia". W praktyce oznacza to konieczność nawigowania w dół struktury. Tym samym dane nie są dostępne z dowolnego poziomu, lecz są zawsze osadzone w kontekście nadrzędnym.

15.Jeszcze inaczej sprawa wygląda w przypadku formatu JSON, który definiuje się jako zbiór par nazw i wartości, gdzie wartością może być kolejny obiekt lub tablica. Taka definicja (obiekt w obiekcie) jest definicją struktury hierarchicznej (drzewiastej).

16.Mając na uwadze, że GROK nakłada wzorzec na pole tekstowe, tj. skanuje tekst od lewej do prawej (liniowo), próbując dopasować znaki, nie będzie właściwy dla struktury danych w postaci tzw. drzewa, co jest niezbędne do poprawnego, nieliniowego parsowania XML czy JSON.

17.Odwołujący w środku odwoławczym podnosi, że:

1)dostarczony przez niego opisu nie stanowi, iż parsowanie musi odbywać się poza środowiskiem graficznym,

2)składnia GROK umożliwia tworzenie "praktycznie dowolnych parserów",

3)gdyby Zamawiający znał GUI, odnalazłby wymagane funkcje pod przyciskiem "Dodaj parser", gent posiada wbudowane funkcje antywirusowe i detekcyjne. Jego obecność w systemie dowodzi, że Odwołujący oferuje rozwiązanie oparte nie tylko o bazę danych, lecz implementuje gotowy produkt pudełkowy (Elastic Security).

Punkt 11 opisu przedmiotu zamówienia

11. Punktem wyjścia dla oceny zgodności oferty jest wykładnia wymagań postawionych przez Zamawiającego. Zgodnie z dokumentami zamówienia, system musiał być wyposażony

4) wymagana jest wiedza o architekturze i dodanie źródła danych (np. urządzenia Syslog), czego Zamawiający nie zrobił, a ponadto źle sprecyzował w jaki sposób będzie weryfikował system – wówczas „można by jakoś to przygotować".

18.Powyższa argumentacja stanowi próbę redefinicji wymagań na etapie postępowania odwoławczego. Odwołujący próbuje zastąpić wymóg posiadania dedykowanych, wcześniej opracowanych narzędzi wymogiem posiadania narzędzia

uniwersalnego (GROK), które przy odpowiednim nakładzie pracy może zrealizować ten sam cel. Jeżeli jednak Zamawiający wymagał obsługi konkretnych formatów poprzez interfejs graficzny, to intencją było pozyskanie systemu, który wykona polecenia względem tych formatów. Formaty te są standardami o ściśle określonej strukturze. Wymaganie ich obsługi w GUI oznacza oczekiwanie, że w operator wybierze z listy wymagany format, a system automatycznie rozpozna strukturę. System Odwołującego, opierający się na mechanizmie GROK, zmusiłby Zamawiającego do ręcznego definiowania struktury za pomocą wzorców tekstowych do tego niededykowanych. Nie jest to gotowy parser w GUI, lecz edytor kodu w GUI.

19.Zamawiający oczekiwał próbki systemu w celu potwierdzenia jego zgodności z wymaganiami. Zatem w Postępowaniu próbka jest materializacją oświadczenia woli Odwołującego. Ma ona pokazywać stan systemu w momencie składania ofert. Jeżeli w trakcie weryfikacji próbki Zamawiający nie znalazł funkcjonalności wymaganych, a Odwołujący nie był w stanie ich wskazać podczas prezentacji, to zgodnie z pkt 144 opisu przedmiotu zamówienia stanowi to dowód tego, że oferta pozostaje niezgodna z wymaganiami Zamawiającego.

20.Argumentację Odwołującego, że funkcje te można „jakoś przygotować" gdyby Zamawiający sprecyzował sposób weryfikacji, należy uznać za nieskuteczną. Po pierwsze próbka nie może być półproduktem, zapowiedzią dopiero wytworzenia funkcjonalności na etapie wdrożenia. System w wersji testowej powinien posiadać gotowe rozwiązania dla określonych wymogów, przykładowo widoczne w interfejsie jako opcje wyboru. Brak tych opcji jest dowodem, którego nie można zastąpić ogólnikowymi zapewnieniami o potencjale konfiguracyjnym systemu w przyszłości.

21.Ponadto Zamawiający nie doprowadził do sytuacji, w której ujawniłby lub uzgodnił sposób weryfikacji, żeby Odwołujący mógł przygotować system pod konkretne, wcześniej wyspecyfikowane czynności. To rolą Odwołującego było zaoferowane systemu spełniającego wymagania, w tym przygotowanie i opisanie scenariuszy, które umożliwią Zamawiającemu ich samodzielną weryfikację, niepoprzedzoną konsultacjami. Odwołujący natomiast próbuje przerzucić odpowiedzialność na Zamawiającego, zarzucając mu brak wiedzy o architekturze. Jest to próba obrony niezasługująca na uwzględnienie. To Odwołujący jako profesjonalista, zobowiązany jest przygotować ofertę, próbkę i scenariusze testowe w sposób, który umożliwi Zamawiającemu jednoznaczną weryfikację spełnienia wymagań.

22.Jeżeli obsługa formatu SYSLOG wymagała dodania źródła logów, Odwołujący powinien był przygotować próbkę systemu w taki sposób, aby weryfikacja była w ogóle możliwa. Obrona swojego produktu polegająca na zarzucaniu Zamawiającemu braku możliwości dodania źródła logów, wzmacniając to stwierdzeniem o braku wiedzy nt. architektury systemu iS Sec, jest argumentacją absurdalną i pozbawioną logiki. Zamawiający ponownie przypomina i podkreśla, że to rolą Odwołującego było wykazanie spełnienia wymagań poprzez udostępnienie systemu i opisanie scenariuszy, które wykażą spełnienie tych wymagań. Odwołujący nie wywiązał się z tej roli ani na etapie składania ofert, ani w toku spotkania zorganizowanego po przekazaniu uwag (por. pkt. 75-78)

Punkt 23 opisu przedmiotu zamówienia

23.Wymogiem Zamawiającego względem systemu w zakresie elektronicznej dokumentacji była możliwość wizualizacji w formie interaktywnej mapy sieci, gdzie na pierwszym planie będą widoczne urządzenia zabezpieczeń, strefy bezpieczeństwa oraz połączenia sieciowe wskazujące jakie mechanizmy zabezpieczeń chronią poszczególne strefy bezpieczeństwa. Zamawiający oczekiwał, że „kliknięcie" na dowolny z obiektów na pierwszym planie pozwoli na podgląd oraz edycję parametrów tego obiektu. Przykładowo po kliknięciu na strefę bezpieczeństwa musi istnieć możliwość definiowania komputerów należących do tej strefy, ich adresacji oraz innych z nimi związanych parametrów.

24.Tymczasem Odwołujący zarzuca, że opis przedmiotu zamówienia nie precyzował wymogów co do rozdzielczości mapy. Twierdzi, że „rozdzielczość mapy (...) może być zmieniona wg wytycznych zamawiającego w procesie konfiguracji" (podkreślenie Zamawiającego) oraz że Odwołujący jest w stanie „skonfigurować system tak, żeby np. ta mapa była wyświetlana w osobnym oknie na całości ekranu" (podkreślenie Zamawiającego). Ostatecznie Odwołujący argumentuje również, że mapa jest czytelna dzięki funkcji „zoom" (przybliżanie scrollem).

25.Analiza dostarczonej próbki wykazała stan zgoła odmienny od deklaracji Odwołującego. Po pierwsze, prezentowana w próbce mapa sieci została zaimplementowana w sztywnych wymiarach 966x800 pikseli. Okno nie skalowało się (nie było responsywne) względem rozdzielczości monitora, zajmując jedynie ok. 27% powierzchni ekranu roboczego (na monitorze o rozdzielczości 2560x1440). Po drugie, w interfejsie próbki systemu brak było widocznej i dostępnej dla użytkownika opcji „wyświetlenia w osobnym oknie na całości ekranu", o której Odwołujący opisuje w czasie przyszłym w odwołaniu. Zamawiającemu nie było dane na etapie badania ofert skorzystać z deklarowanej funkcji. Po trzecie, obsługa mapy w tak małym oknie, przy dużej liczbie obiektów wymusza ciągłe, nieergonomiczne przewijanie i skalowanie, co czyni widok nieczytelnym, a przez to nieintuicyjnym.

26.Zgodnie z pkt. 144 opisu przedmiotu zamówienia, Zamawiający oceniał dostarczoną próbkę systemu, a nie hipotetyczne funkcjonalności, które Odwołujący „może skonfigurować" po wdrożeniu. Próbka w dniu badania posiadała wadę w postaci sztywnego, małego okna wizualizacji, co obniżało jej użyteczność i uzasadniało dokonaną ocenę. Deklaracje Odwołującego o możliwości przyszłej konfiguracji są bezprzedmiotowe w świetle oceny stanu zastanego

próbki.
Punkt 51 opisu przedmiotu zamówienia
27.Na wstępie Zamawiający, referując do stwierdzenia Odwołującego dot. braku wiedzy Zamawiającego na temat systemu, technologii oraz ogólnej zasady działania tego typu systemów, za zasadne uważa przywołanie stanowiska wyrażonego w pkt. 6 i 19-21 również w tym miejscu odpowiedzi.
28.Odnosząc się do uwag Odwołującego dot. języka angielskiego oraz wiedzy co do pól zaimplementowanych w systemie, Zamawiający wskazuje, co następuje. W pierwszej kolejności należy zwrócić uwagę na listę pól dostępnych do budowy reguł, która nie jest posortowana ani alfabetycznie, ani według logicznych grup systemowych. Wymaga to od użytkownika żmudnego przeszukiwania listy „linijka po linijce". Po drugie, system wyświetla jedynie nazwy techniczne pól, bez żadnych podpowiedzi. Widoczne są pola takie jak elastic_agent.id.keyword czy ds-logs-filestream (gdzie pojęcie „wzorzec" raz występuje po polsku, a raz jako „pattern"), których znaczenie nie jest wyjaśnione w interfejsie ani w dostarczonej dokumentacji. Po trzecie, na liście wyboru znajdują się pola o nazwach wieloznacznych, np. related.ip. Interfejs nie informuje, czy pole to dotyczy adresu IPv4 czy IPv6. Zmusza to użytkownika do domyślania się lub zewnętrznej weryfikacji w dokumentacji silnika Elastic (co potwierdza oparcie systemu o rozwiązania osób trzecich, a nie autorską, spójną logikę).
29.Odwołujący w odwołaniu wprost przyznaje, że „można było się domyślić z jakich systemów pochodzą". Taka konstrukcja interfejsu stoi w sprzeczności z definicją intuicyjności, która zakłada łatwość obsługi bez konieczności domyślania się ukrytych znaczeń.
30.Podsumowując, obniżona ocena intuicyjności nie wynikała z samego użycia języka angielskiego, lecz z chaosu organizacyjnego w interfejsie, braku kategoryzacji pól oraz braku opisów funkcjonalnych, co czyni proces tworzenia reguł podatnym na błędy i czasochłonnym. Na dowód powyższego Zamawiającego przedstawia nagranie z badania próbki systemu, który potwierdza, że interfejs wymaga od operatora posiadania wiedzy tajemnej, bo niedostępnej w systemie ani instrukcji, a nie wiedzy inżynierskiej (plik „Reguły korelacyjne IS Sec,mkv", czas: od 1:43 do 2:22, od 4:06 do 7:28).
31.Na marginesie, nawiązując do niemerytorycznych uwag Odwołującego podważających kompetencje personelu IT Zamawiającego, należy wskazać, że stanowią one niedopuszczalną w profesjonalnym obrocie próbę odwrócenia uwagi od wad oferowanego systemu. Fakt, że Odwołujący uzależnia obsługę systemu od „domyślania się" (co wprost przyznaje w odwołaniu) oraz posiadania przez operatora systemu niemalże wiedzy tajemnej, nieopisanej w dokumentacji ani instrukcji, dowodzi nieintuicyjności oferowanego narzędzia, a nie braku wiedzy Zamawiającego. Pozbawiona taktu narracja ad personam nie zastąpi brakującej funkcjonalności systemu, nie wchodzi zakres ochrony prawnej, stanowi dowód braku kultury i przez to zasługuje na pogardę.
32.Przechodząc do możliwości stosowania atrybutów użytkowników i komputerów z Active Directory, Zamawiający podtrzymuje dokonaną ocenę i stoi na stanowisku, że system nie spełniał ww. wymogu. Na prezentowanym przez Odwołującego zrzucie ekranu (s. 24) widnieją takie pozycje jak:
1)o365.audit.Parameters.WorkDays,
2)o365.audit.ModifiedPropertiesDevice,
3)o365.audit.CorrelationId,
4)winlog.event_data.Schema.keyword,
5)winlog.proces.pid,
6)winlog.event_data.ReturnCode.key.
33.Wymienione pozycje pochodzą z dzienników zdarzeń systemowych i zawierają informacje dostępne w momencie i miejscu zdarzenia. Są one statyczne względem zdarzenia – nie zmieniają się wraz ze zmianami stanu Active Directory. Filtry oparte na winlog.event_data i o365.audit zawierają wyłącznie dane dostępne w samych logach.
34.W tym miejscu należy wyjaśnić, że Active Directory to centralna baza danych, która nadaje tożsamość logom. Obrazując to przykładem, o ile log informuje, że „użytkownik X zalogował się na komputerze Y", o tyle atrybuty Active Directory precyzują, że „użytkownik X jest Dyrektorem Finansowym, a komputer Y to serwer przechowujący dane wrażliwe". Zamawiający wymagał, aby te konkretne informacje były bezpośrednio dostępne jako gotowe pola.
35.System Odwołującego dostarcza jedynie technicznych parametrów technologii Windows (np. numer procesu, kod błędu). Są to dane techniczne, oparte na zdarzeniach, ale nie zawierają w sobie informacji o tym, kim jest dany użytkownik w badanej strukturze. Zamawiający natomiast wymagał, żeby system posiadał dostęp do szczegółowych danych, takich jak: przynależność do grupy (np. „Administratorzy"), dział (np. „Kadry"), czy lokalizacja komputera.
36.Odwołujący w dostarczonej próbce systemu nie zaimplementował Active Directory, co było wymagane w punktach 51c i 51d opisu przedmiotu zamówienia. Zaoferowanie dostępu do logów systemowych jest jedynie warunkiem koniecznym do działania systemu, ale niewystarczającym do spełnienia wymogu wykorzystania atrybutów AD w procesie korelacji odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie.
37.Odnosząc się do twierdzenia Odwołującego odnośnie modułów UEBA oraz wskaźnika kompromitacji IoC i „niechęci

sprawdzenia (przeklikania systemu) oraz brak wiedzy na jego temat oraz tego typu technologii i systemów uniemożliwił Zamawiającemu odnalezienie tych funkcjonalności", należy wskazać, że Odwołujący nie pokazał na żadnym zrzucie ekranu (a wcześniej w próbce) modułów zarządzania IoC ani UEBA. Instrukcja obsługi zawierała rozdział „Reguły korelacyjne", który nie zawierał żadnej treści– poniżej fragment instrukcji dostarczonej przez Odwołującego:

38.Z kolei scenariusz testowy tej funkcji ograniczył się do wskazania okna reguł korelacyjnych i zdania „Przeglądnij dostępne opcje". Twierdzenie, że system posiada w/w moduły, bez ich zaprezentowania w próbce, jest gołosłowne. Przenosząc zasadę ciężaru dowodu na grunt niniejszej sprawy, elementy nieujęte w próbce, uznaje się za nieistniejące w ofercie.

Punkt 72 opisu przedmiotu zamówienia

39.Zamawiający zweryfikował każdą ze wskazanych zakładek, wykonując i dokumentując scenariusz testowy przedstawiony przez Odwołującego. Wynik tej weryfikacji, widoczny na całym przebiegu nagrania (por. Przypisywanie automatyczne zdarzeń IS Sec.mkv) nie ujawnił istnienia jakichkolwiek mechanizmów konfiguracji „logiki automatycznego przypisywania" opartej na wymaganiach z opisu przedmiotu zamówienia, tj. dostępności operatora czy jego bieżącego obciążenia.

40.Weryfikacja instrukcji obsługi, na którą powołuje się Odwołujący, wykazała, że na stronach 64-84 opisane są wyłącznie reguły powiadamiania (notyfikacji), a nie przypisywania zgłoszeń do konkretnego operatora w oparciu o obciążenie bądź dostępność (por. pkt 72 zd. 2 opisu przedmiotu zamówienia).

41.Twierdzenie Odwołującego, jakoby automatyczne przypisanie polegało na wyświetleniu zdarzeń zalogowanemu użytkownikowi, jest próbą wprowadzenia w błąd. Opis przedmiotu zamówienia w pkt. 72 definiuje, że system musi posiadać logikę uwzględniającą „dostępność operatora" i „jego obciążenie". Mechanizm polegający na wyświetleniu wszystkich zdarzeń z racji posiadania jednego konta, a na tym koncie uprawnień administratora, nie jest logiką przypisywania zadań, lecz ich prezentacją.

42.Ponownie, twierdzenie o rzekomej niekompetencji Zamawiającego pozostaje bezzasadne w świetle dowodu z nagrania, na którym widać jak Zamawiający realizuje krok po kroku scenariusz testowania dostarczony przez Odwołującego. Uszło uwadze Odwołującego, że celem instrukcji i scenariusza testowego w procedurze weryfikacji próbki jest wskazanie Zamawiającemu, gdzie znajduje się wymagana funkcjonalność. Jeżeli funkcjonalność ta nie znajduje się w tych miejscach systemu, do których Zamawiający dotarł w sposób opisany w instrukcji i scenariuszu, to odpowiedzialność za ten stan rzeczy spoczywa wyłącznie ich autor. Braki w instrukcji, jej błędna redakcja lub wskazanie błędnych ścieżek dotarcia do pożądanych funkcji obciążają Odwołującego jako podmiot profesjonalny, zobowiązany do udowodnienia spełnienia wymogów. Ocena znajomości technologii przez Zamawiającego jest subiektywną opinią Odwołującego i nie ma znaczenia w procedurze, w której Zamawiający wykonuje polecenia z instrukcji. To Odwołujący swoim zaniedbaniem uniemożliwił weryfikację poprzez dostarczenie błędnej instrukcji, co potwierdza materiał wideo.

43.Nie sposób nie odnieść się również do tej części odwołania, w której Odwołujący argumentuje w oparciu o przyznanie dostępu do jednego konta (operatora), „do którego automatycznie system przypisał wszystkie zdarzenia/incydenty", co miało na celu przedstawienie funkcjonalności. Otóż, jeśli Odwołujący skonfigurował tylko jedno konto, czym – jak sam przyznaje – technicznie uniemożliwił prezentację mechanizmu podziału zadań, to jest to okoliczność obciążająca wyłącznie Odwołującego. Zamawiający nie może domniemywać działania funkcji, której nie można uruchomić z powodu ograniczeń konfiguracyjnych narzuconych przez dostawcę próbki. Automatyczne przypisanie wszystkich procesów do jedynego użytkownika nie jest realizacją algorytmu badanego obciążenia i dostępności, lecz domyślnym zachowaniem każdego systemu informatycznego przy braku innych użytkowników. Tak skonfigurowana próbka prezentująca możliwości systemu nie może zostać uznana za spełniająca w/w wymóg.

Punkt 75 opisu przedmiotu zamówienia

44.Odwołujący podnosi, że opis przedmiotu zamówienia nie precyzował sposobu realizacji funkcjonalności grupowania. Zdaniem Odwołującego zastosowanie przycisku „przypisz zdarzenie" jest rozwiązaniem wystarczającym i intuicyjnym, a ocena Zamawiającego w tym zakresie jest nierzetelna. Ponadto Odwołujący deklaruje gotowość zmiany nazwy funkcji na etapie wdrożenia.

45.Jednak z twierdzeniami Odwołującego nie sposób się zgodzić, a wynik oceny Zamawiającego potwierdza materiał dowodowy w postaci nagrania (plik Przypisywanie zdarzeń IS Sec.mkv). Jak prezentuje nagranie, czynność „przypisania" incydentu nie polega na wyborze incydentu z listy bądź zaznaczenie incydentu/incydentów i wykonanie polecenia, lecz wymaga ręcznego przepisania 32-znakowego unikalnego identyfikatora zdarzenia nadrzędnego i przypisanie do zdarzenia podrzędnym (bądź incydentu podrzędnego do nadrzędnego). Zamawiający zwraca uwagę, że w toku badania, w warunkach „laboratoryjnych" (brak presji czasu i stresu towarzyszącego incydentom krytycznym, gdzie czas ich zażegnania może wpłynąć na rozmiar szkody), pracownik Zamawiającego dwukrotnie popełnił błąd podczas przepisywania ciągu znaków, co nie powinno dziwić biorąc pod uwagę, że jest to ciąg znaków składających z liter i cyfr.

Potwierdza to, że zaimplementowana metoda jest nieergonomiczna i stwarza realne zagrożenie dla ciągłości obsługi incydentów.

46.Co więcej, w końcowej fazie nagrania widoczne jest, że system nie posiadał (lub instrukcja nie kierowała do tej czynności) funkcjonalności umożliwiającej zamknięcie incydentu nadrzędnego w sposób, który wymusiłby automatyczne zamknięcie incydentów podrzędnych. Dla przypomnienia, opis przedmiotu zamówienia stanowił, że: „zamknięcie nadrzędnego zdarzenia musi zamykać też wszystkie podrzędne".

47.W ocenie Zamawiającego powyżej opisany i nagrany sposób obsługi incydentów dobitnie pokazuje jak nieintuicyjny, a nawet niebezpieczny biorąc pod uwagę wykorzystanie systemu w sytuacjach zagrożenia, pozostaje oferowany system Odwołującego. Polemika Odwołującego z gustem Zamawiającego jest tylko odwróceniem uwagi od realnego problemu, jaki mógłby stworzyć oferowany system.

Punkt 87 opisu przedmiotu zamówienia

48.Zamawiający ponownie przypomina, że to na Odwołującym spoczywał obowiązek przygotowania systemu i instrukcji w sposób niebudzący wątpliwości. Zamawiający nie jest zobowiązany do poszukiwania ukrytych funkcjonalności systemu ani do domyślania się sposobu ich działania, jeżeli nie wynika to wprost z dostarczonej instrukcji (scenariusza testowania).

49.Odwołujący zarzuca Zamawiającemu, że ten nie zaznajomił się z jego prostym opisem. Należy jednak zauważyć, że polecenie w instrukcji brzmiało lakonicznie: „5. Sprawdź możliwości filtrowania wyników". Taka redakcja instrukcji przenosi ciężar eksploracji na Zamawiającego, ale z konsekwencjami dla Odwołującego. Instrukcja powinna wskazywać konkretną ścieżkę kliknięć prowadzącą do uzyskania wymaganego efektu. Brak takiej precyzji obciąża jedynie Odwołującego.

50.Aby wyjaśnić istotę problemu, warto wyjaśnić różnicę pomiędzy funkcją filtrowania (wymaganą przez Zamawiającego) a funkcją wyszukiwania (oferowaną przez Odwołującego). Wykonawca opiera zarzut na tezie, że system posiada wyszukiwarkę oraz moduł analizy podatności, które konsumują wymaganie filtrowania.

51.Otóż wyszukiwanie jako czynność polega na odnalezieniu konkretnego wyniku (lub grupy grupy) na podstawie dopasowania ciągu znaków (słów kluczowych) do treści przechowywanych w bazie danych. Użytkownik wpisując poszukiwany wynik oczekuje, że system przeszuka bazę w poszukiwaniu wystąpień tej frazy. Z kolei filtrowanie polega na zawężeniu widocznego zbioru poprzez parametry co do zdefiniowanych uprzednio właściwości. Filtrowanie opiera się na strukturze i typach danych: rozróżnia daty, liczby, statusy, co pozwala na odnalezienie wyników z pożądanego zakresu, których zwykła wyszukiwarka tekstowa nie wykona.

52.Zamawiający, po wykonaniu czynności wskazanych w dostarczonym scenariuszu testowym, po wejściu we wskazaną zakładkę „Podatności", spotkał się z listą zawierającą wyłącznie jedną podatność. W oknie nie był widoczny żaden panel boczny, menu kontekstowe ani zestaw filtrów umożliwiających selekcję danych wg kryteriów z pkt. 87. Widoczny interfejs nie oferował funkcjonalności pozwalających na zawężanie wyników w sposób wymagany.

53.Należy podkreślić, że umieszczenie wyników skanowania podatności w module SLA jest informatycznym absurdem i dowodzi braku logiki w architekturze systemu. Aby uzmysłowić skalę tego absurdu, należy najpierw wyjaśnić czym jest SLA i zarządzanie podatnościami.

54.SLA (Service Level Agreement) to moduł służący do monitorowania jakości świadczenia usług. Dotyczy parametrów opartych na czasie, takich jak dostępność systemu, czas reakcji na zgłoszenie, czas usunięcia awarii. Z kolei zarządzanie podatnościami jest modułem służącym do identyfikacji, oceny i eliminacji luk bezpieczeństwa.

55.W systemie Odwołującego, aby odnaleźć listę podatności, operator musi udać się do modułu służącego do rozliczania umów i czasów reakcji (SLA). Jest to działanie sprzeczne z jakąkolwiek intuicją i logiką, zwłaszcza że w głównym menu jest zakładka „Skaner podatności". Ulokowanie funkcji z zakresu bezpieczeństwa w module rozliczeniowym sprawia, że dla użytkownika końcowego funkcja ta jest de facto niedostępna. Zamawiający nie ma obowiązku badania całego systemu w poszukiwaniu pożądanych funkcji, które Odwołujący ukrył w nielogicznych lokalizacjach, ale co gorsze - nie opisał w dostarczonych materiałach, pozostawiając Zamawiającego bez wymaganego wsparcia.

Punkt 122 opisu przedmiotu zamówienia

56.Zamawiający wymagał, aby rozwiązanie SIEM wspierało obsługę agentów na systemy Windows, posiadających m.in. centralne zarządzanie i możliwość aktualizacji z głównej konsoli (lit. a); zdolność monitorowania integralności plików, rejestru systemowego oraz urządzeń zewnętrznych (lit. d, e, f); możliwość przygotowania i przypisywania różnych zestawów konfiguracji (lit. i); automatyzację reakcji (blokowanie ruchu/procesu) - lit. j.

57.Odwołujący twierdzi, że system posiada agentów, których zarządzanie jest możliwe w "formie uproszczonej" (sprawdzanie statusów/usuwanie), a aktualizacja i reakcja odbywają się poprzez skrypty w module SOAR ("Playbooki"). Zarzuca Zamawiającemu,

że ten pominął instrukcję nakazującą szukanie funkcji agentowych w module automatyzacji (SOAR).

58.Weryfikacja systemu Odwołującego, utrwalona na nagraniu wideo (por. plik Agenty IS Sec.mkv), potwierdza prawidłowość oceny dokonanej na etapie badania próbki.
59.Nawiązując do pkt. 122 lit. a opisu przedmiotu zamówienia, zgodnie z instrukcją Odwołującego, użytkownik jest kierowany do modułu SOAR -> Playbooki. Jest to próba obejścia wymogu. Moduł SOAR służy do orkiestracji incydentów (łączenie rozproszonych systemów bezpieczeństwa takich jak firewalle, systemy SIEM, poczta elektroniczna, w jeden spójny ekosystem, umożliwiając im wymianę informacji), a nie do zarządzania infrastrukturą. Na nagraniu widać listę playbooków (predefiniowane scenariusze, czas 1:49), jednak brak jest tam funkcji służącej do ustalenia: miejsca instalacji agenta, wersji agenta czy mechanizmu dystrybucji aktualizacji na końcówki. System nie posiada narzędzia do zarządzania agentami. Cały scenariusz testowy nie dotyczył agentów system Windows.
60.System był pozbawiony funkcji monitorowania, wymaganych w pkt. 122 lit. d, e, f. W oparciu o próbę nie stwierdzono żadnych opcji konfiguracji monitorowania integralności plików, rejestru systemowego ani urządzeń zewnętrznych (np. nośników danych). W sekcji "Lista urządzeń" widocznej na nagraniu brak jest wglądu w jakiekolwiek parametry, a jedyne informacje to wersja systemu operacyjnego i adres IP (czas 3:00). Świadczy to o tym, że istnieje komunikacja zwrotna z agentem. Fakt ten jednak w żaden sposób nie dowodzi spełnienia w/w wymagań. Sama bowiem obecność agenta raportującego wersję systemu nie jest tożsama z posiadaniem przez niego wymaganych funkcji. Jak prezentuje dostarczone nagranie, nie stwierdzono żadnych danych ani opcji konfiguracyjnych potwierdzających monitorowanie zmian w plikach, rejestrze czy podłączenia nośników zewnętrznych.
61.Pomimo wymogu dot. komunikacji z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystałem protokołu HTTPS (por. pkt 122 lit. g opisu przedmiotu zamówienia), w systemie nie ma przykładowo sekcji zarządzania certyfikatami szyfrującymi połączenie dla agentów ani podglądu statusu szyfrowania bądź inny dowolny dowód, że połączenie jest szyfrowane. Dostarczony scenariusz testowania w żaden sposób nie umożliwiał ustalenia, że połączenie było zaszyfrowane.
62.Odnośnie możliwości monitorowania stanu agentów w konsoli zarządzającej, sama lista urządzeń nie potwierdza spełnienie wymogu. To, że system widzi komputer w sieci (np. odpowiada na polecenie PING), nie oznacza, że zainstalowany na nim agent działa poprawnie, jest aktywny i przesyła logi. Prezentowana w systemie lista to nic innego jak widoczne zasoby sieciowe, a nie konsola zarządzania agentami. Widoczne statusy i informacje (online/active, adres IP) odnoszą się wyłącznie do dostępności sieciowej. Nagranie we fragmencie prezentującym urządzenia w sieci ujawnia, że system nie rozróżnia sytuacji, w której komputer jest włączony, ale np. proces agenta uległ zatrzymaniu. Widoczność urządzenia w sieci nie jest tożsama z monitorowaniem stanu agenta. Wymóg dotyczył weryfikacji, czy oprogramowanie zabezpieczające działa, a nie czy komputer jest podłączony do zasilania.
Próbka systemu nie wykazała możliwości tworzenia zestawów polityk (np. osobna polityka dla DNS, osobna dla AD) i ich zdalnego przydzielania grupom agentów (por. pkt 122 lit. i opisu przedmiotu zamówienia).
Punkt 125 opisu przedmiotu zamówienia
63.W odpowiedzi na wezwanie Zamawiającego, Odwołujący udostępnił środowisko demonstracyjne systemu iS Sec, opartego na silniku Elastic Search i MS SQL. Odwołujący wprost wskazał w scenariuszu testowym: „System jest zintegrowany z zewnętrznymi bazami danych Threat Inteligence". Weryfikacja przeprowadzona przez Zamawiającego ujawniła jednak rozbieżność pomiędzy oświadczeniem a stanem faktycznym.
64.Po pierwsze przedstawiony do testów system nie zawierał możliwości konfiguracji API do zewnętrznych dostawców Threat Inteligence Feed. Zamiast dynamicznie pobieranej bazy danych ze źródeł typu open source lub komercyjnych, „baza" Odwołującego zawierała statyczną listę 10 plików. Na marginesie Zamawiający uważa za uzasadnione wyjaśnienie, że baza jest określeniem oczywiście przesadzonym, bowiem analiza wpisów w bazie danych wykazała manualne, testowe wprowadzenie 10 plików, przy czym pliki te przyjęły nazwy zawierające słowa „test" lub „testowy", a także nazwane pojedynczymi literami sąsiadującymi na klawiaturze (co sugeruje przypadkowe naciśnięcia klawiszy przez Odwołującego w toku wprowadzania danych), oraz – co najważniejsze – wpisy, w których hash był identyczny dla trzech różnych plików. Wyjaśniając zagadnienie identycznego hash'u plików: w przypadku plików tekstowych identyczny hash oznacza tyle, że pliki tekstowe – choć o różnej nazwie – zawierają identyczne każde zdanie, słowo, znak interpunkcyjny, formatowanie czy ukryty znacznik wewnątrz pliku.
65.Odwołujący w treści pisma zarzuca Zamawiającemu nierzetelność weryfikacji, twierdząc, że ten zaniechał sprawdzenia, co znajduje się w Module Threat Intelligence. Odwołujący powołuje się na scenariusz testowy (punkty 2 i 3: „Przeglądnij bazę wiedzy...", „Sprawdź listę blokowanych plików"), sugerując, że sama obecność modułu i jakichkolwiek danych (nie mylić z bazą danych – por. pkt 64) w nim zawartych dowodzi spełnienia wymogu integracji. Odwołujący ostatecznie zarzuca Zamawiającemu złą wolę lub brak wiedzy. Zamawiający pragnie wyjaśnić, że pojęcie Threat Intelligence Feed oznacza ciągły, zautomatyzowany strumień danych dostarczający w czasie rzeczywistym informacji o potencjalnych i aktualnych zagrożeniach. Przeciwieństwem tego pojęcia jest z pewnością statyczna lista plików zaoferowana Zamawiającemu do testów, imitująca bazę danych. Obecność plików o nazwach „test" oraz pliki o

identycznych hash'ach stanowi dowód na to, że dane te zostały wprowadzone ręcznie przez Odwołującego, a nie pobrane z bazy dostawców. Świadczy to o tym, że moduł w próbce był jedynie atrapą pozbawioną realnej wartości testowej i świadczącej o systemie iS Sec jako całości. Zamawiający wymagał w opisie przedmiotu zamówienia, aby system zawierał zintegrowany zestaw baz zagrożeń.

66.Zamawiający pragnie jeszcze powrócić do twierdzenia Odwołującego, że Zamawiający nie wykonał pkt. 2 i 3 scenariusza: „Wybierz z menu Moduł Threat Inteliligence", „Przeglądnij bazę wiedzy z różnych kategorii danych" (pisownia oryginalna). Otóż Zamawiający dokonał tych czynności i to właśnie one ujawniły brak integracji, oraz brak zintegrowanego zestawu baz zagrożeń. Odwołujący pozostaje w błędzie twierdząc, że samo wyświetlenie listy plików w interfejsie dowodzi integracji z zewnętrznymi bazami. Stanowi to dowód przeciwny, bowiem Zamawiający wymagał zintegrowania z zewnętrznymi bazami, co powinno doprowadzić do wymiany danych. Skoro baza zawierała statyczne pliki testowe, to proces wymiany danych nie zachodził i nie miała miejsce czynność „integracji", co obnaża próbkę systemu jako nieprzygotowaną do wykazania spełnienia wymagań.

67.Zamawiający zwraca dodatkowo uwagę, że Odwołujący dopuścił się manipulacji na etapie postępowania odwoławczego, przedstawiając zmodyfikowany zrzut ekranu systemu względem dostarczonej próbki. Po lewej stronie znajdują się zrzuty ekranu zarejestrowane przez Zamawiającego, po prawej zaś – zrzuty ekranu dołączone do odwołania:

68.Odwołujący w piśmie posługuje się grafikami z innej wersji systemu niż ta udostępniona Zamawiającemu. W dostarczonym nagraniu widać, że Zamawiający próbował wylistować zagrożenia z okresu ponad 5 lat. System nie zwrócił żadnego wyniku, co potwierdza, że „gotowy mechanizm" w rzeczywistości nie działał, tj. w systemie nie było żadnego znanego zagrożenia sieciowego (por. plik Threat Intelligence Feed IS Sec.mkv czas od 0:45 do 1:50).

69.Jak widać na zrzutach ekranu prezentowanych przez Odwołującego, zagrożenia widnieją na dzień 21 grudnia 2025 r., co stanowi podstawę do stwierdzenia, że argumentacja Odwołującego opiera się na wersji systemu nieznanej Zamawiającemu.

Wymaganie opcjonalne nr 2 i punkty 10, 11, 12, 13, 14, 15

70.Odwołujący nie zgadza się z oceną punktów dotyczących funkcjonalności opcjonalnej. Twierdzi, że system iS Sec jest „rozbudowanym systemem posiadającym te wszystkie funkcjonalności", a negatywna ocena wynika ponownie z niewiedzy albo celowego działania Zamawiającego. Na dowód posiadania funkcji Odwołujący załączył do odwołania zrzuty ekranu (str. 39-40), sugerując, że rzetelne przejście scenariusza wykazałoby zgodność.

71.Podczas weryfikacji próbki systemu, Zamawiający stwierdził, że udostępniony moduł nie posiadał cech działającego oprogramowania, a jedynie prezentował statyczne widoki danych testowych. W systemie co prawda widoczne były dane testowe, jednak nie zidentyfikowano żadnego interfejsu ani funkcji umożliwiającej ich edycję, dodawanie nowych rekordów czy import danych z zewnątrz.

72.Dostarczona dokumentacja (instrukcja i scenariusz testowy) nie zawierała informacji o źródle pochodzenia danych widocznych w systemie ani procedury ich wprowadzania. Odwołujący nie wskazał sposobu dotarcia do tych funkcji, co stoi w sprzeczności z obowiązkiem wynikającym z pkt. 145 lit. c OPZ (obowiązek opracowania instrukcji realizacji scenariuszy testowych).

73.Weryfikacja wykazała, że moduł nie realizował wymagań, w szczególności:

1)system nie rejestrował kategorii czynności przetwarzania,

2)nie posiadał narzędzi do inwentaryzacji obszarów przetwarzania (brak wyszukiwania systemów IT, grup i kategorii danych),

3)nie wykonywał automatycznej analizy ryzyka dla zagrożeń informatycznych (poufność, integralność, dostępność),

4)nie pozwalał na określenie konsekwencji dla osób fizycznych w ramach analizy ryzyka,

5)nie generował raportów z oceny skutków dla ochrony danych wymaganych art. 35
RODO ,

6)nie posiadał repozytorium dokumentów z kontrolą wersji i nadzorem nad dostępem.

74.Odnosząc się do prezentowanych w odwołaniu zrzutów ekranu to pozostają one bezprzedmiotowe, gdyż przedstawiają funkcjonalności, które nie były dostępne lub aktywne dla Zamawiającego, ewentualnie nie były dostępne lub aktywne w wyniku wykonania scenariusza testowego Odwołującego.

Brak wyjaśnień Odwołującego w trakcie spotkania

75.Kierując się treścią pkt. 145 opisu przedmiotu zamówienia, doszło do spotkania on-line w celu odniesienia się do wyników oceny zgodności systemu. Spotkanie stanowiło możliwość zajęcia stanowiska przez Odwołującego na ocenę mu ujawnioną jeszcze przed spotkaniem w celu przygotowania się i prezentacji funkcjonalności systemu, których Zamawiający samodzielnie nie był w stanie ustalić w oparciu przekazany mu opis.

76.Niemniej w toku spotkania Odwołujący ograniczył się do gołosłownych twierdzeń i zapewnień, że „system spełnia wymogi OPZ", nie popierając tego żadnym dowodem w postaci prezentacji działania systemu. Odwołujący nie dopuścił do demonstracji systemu na przekazanej próbce i nie zapewnił wymaganego w pkt 145 opisu przedmiotu zamówienia wsparcia technicznego. Na ponawiane przez Zamawiającego pytania dotyczące sposobu wywołania nieodnalezionych

funkcjonalności, Odwołujący nie był w stanie udzielić ani jednej merytorycznej odpowiedzi, która pozwoliłaby na zmianę dotychczasowej oceny.
77.Mimo dobrej woli Zamawiającego i propozycji dotyczącej dołączenia do spotkania innych osób znających system oraz deklaracji przedłużenia spotkania na kolejny dzień roboczy, Odwołujący odmówił, godząc się tym samym z oceną systemu.
78.Zachowanie Odwołującego w toku spotkania Zamawiający uznał za brak odpowiedzi na ocenę przedstawioną mu przed spotkaniem, a w konsekwencji potwierdzenie, że zaoferowany system nie spełnia wymagań określonych w opisie przedmiotu zamówienia.
II.Zarzut dotyczący naruszenia art. 226 ust. 1 pkt 8) w zw. z art. 224 ust. 6 Ustawy (…)
79.Odwołujący w swoim środku odwoławczym próbuje przenieść ciężar dowodu na Zamawiającego, zarzucając mu „domniemanie" argumentów. Jest to zarzut niezasługujący na uwagę z tego powodu, że to Odwołujący, w odpowiedzi na konkretny zakres wezwania, miał obowiązek przedstawić dowody na twierdzenia, które tam zawarł. Odwołujący temu obowiązkowi nie sprostał, ograniczając się do ogólnych deklaracji i quasi dowodów, bo o charakterze poglądowym, a nie faktycznym.
80.Ustawodawca w art. 224 ust. 1 Ustawy wskazuje wprost na obowiązek złożenia „wyjaśnień, w tym złożenia dowodów". Użycie liczby mnogiej oraz sformułowania „w tym" sugeruje, że same twierdzenia, przyjmujące postać wyjaśnień, są niewystarczające, jeśli nie towarzyszą im dowody. Jeśli chodzi o dowody to można wyróżnić dowody odnoszące się do konkretnej sytuacji faktycznej, jak oferty podwykonawców, umowy o pracę, faktury, a także dowody abstrakcyjne: statystyki rynkowe, ogólne cenniki internetowe. W sprawach dotyczących rażąco niskiej ceny wartość dowodowa tych drugich jest znikoma. Zamawiający bada bowiem sytuację konkretnego wykonawcy w konkretnym postępowaniu, oferującego wykonanie zamówienia za konkretną cenę lub koszt, a nie średnią rynkową.
81.W zawisłej sprawie Odwołujący jako jedyny dowód na realność przyjętych stawek dla dwóch osób przedstawił zrzuty ekranu z portalu wynagrodzenia.pl. Jest to przykład dowodu abstrakcyjnego, który nie potwierdza, że Odwołujący faktycznie ponosi takie koszty, a jedynie, że w Internecie można znaleźć określone dane. Akceptacja takiego „dowodu" prowadziłaby do wypaczenia sensu postępowania dowodowego, gdyż każdy wykonawca mógłby uzasadnić dowolnie niską cenę, znajdując w Internecie odpowiednio niską stawkę w widełkach, bez względu na to, czy realnie zatrudnia pracowników za takie wynagrodzenie. Zamawiający intencjonalnie odstąpił od posługiwania się przymiotem „statystycznych", bowiem źródło danych wspomnianego portalu jest nieznane.
82.Pozostając jeszcze w temacie wynagrodzeń, jednym z elementów kalkulacji ceny w usługach IT są koszty pracy, bowiem są to przede wszystkim świadczenia niematerialne. Zamawiający w wezwaniu do wyjaśnień żądał podania liczby i kwalifikacji osób oddelegowanych do realizacji zamówienia. W odpowiedzi Odwołujący posłużył się sformułowaniem o posiadaniu „grona specjalistów", „zaangażowaniu zasobów kadrowych", nie precyzując jednak informacji na ich temat, które pozwoliłyby na weryfikację kosztów. Stwierdzenie o „gronie specjalistów" nie jest nośnikiem jakiejkolwiek informacji: czy Odwołujący miał na myśli starszego specjalistę ds. wdrożeń bądź programistę, wynagrodzenia których wskazał w wyjaśnieniach, a może osoby zajmujące jeszcze inne stanowiska. To oraz liczba tych osób pozostają nieznane. Nieznane pozostaje również, jaki jest ich wymiar etatu dedykowany do tego projektu, jaki stosunek prawny wiąże Odwołującego z tą osobą bądź osobami. Złożone przez Odwołującego zrzuty ekranu z portalu wynagrodzenia.pl jako jedyny dowód na wysokość kosztów pracy nie mogą być dowodem, bowiem mają charakter jedynie statystyczny: dane z portalu prezentują średnie lub mediany rynkowe. Nie dowodzą one, że Odwołujący – jako konkretny podmiot gospodarczy – ma zawarte umowy z pracownikami lub biorącymi zlecenie na takich warunkach. Poziom ogólności złożonych wyjaśnień osiągnął niebezpiecznie wysoki poziom.
83.Informacja na temat osób planowanych do zaangażowania zamówienia, w zestawieniu z informacją o czasie realizacji (90 dni, por. § 2 ust. 1 wzoru umowy), jest informacją mającą wpływ na koszt po stronie Odwołującego, a z perspektywy Zamawiającego – informacją istotną z punktu widzenia realności wykonania zamówienia. Dostawa i wdrożenie systemu bezpieczeństwa, realizowanych w wymagającym wymiarze czasu, powoduje zrównoleglenie prac. Brak wskazania konkretnej liczby osób i ich kwalifikacji uniemożliwia Zamawiającemu ocenę, czy cena oferty jest realna. W niniejszej sprawie, powoływanie się na anonimowe „grono" bez pokrycia w liczbach i kosztach jest jedynie technicznym wykonaniem wezwania do złożenia wyjaśnień. W ocenie Zamawiającego nie jest możliwe wykonanie wszystkich czynności w sposób sekwencyjny przez jedną bądź dwie osoby. Stanowi to potwierdzenie tego, że brak informacji o liczbie i kwalifikacjach kadry dedykowanej do wykonania zamówienia, był okolicznością obciążającą Odwołującego.
84.Odwołujący, zamiast przedstawić przykładowo zanonimizowane umowy o pracę (lub inny rodzaj umów), raporty ZUS czy listy płac, posłużył się wydrukami internetowymi. W obliczu ciężaru dowodu było to zaniechanie skutkujące koniecznością odrzucenia oferty. Odwołujący nie udowodnił realności ceny, a jedynie pokazał, jakie koszty ponoszą inni (statystyczni) przedsiębiorcy.

85.Zamawiający w treści wezwania wymagał podania adresu i licencji, z których będą pobierane wymagane dane do systemu. Odwołujący wyjaśnił, że w zakresie baz danych, z którymi łączy się system, bazy te są ogólnie dostępne, ale ich podanie nie było wymagane w treści specyfikacji, a stanowi tajemnicę przedsiębiorstwa Odwołującego. W oparciu o taką informację Zamawiający nie był w stanie ustalić choćby tego, czy dostęp do baz danych jest bezpłatny, czy też wymaga poniesienia kosztu – a jeśli tak, to w jakiej wysokości. Odwołujący zdaje się przeoczył, że ubiega się o udzielenie zamówienia publicznego, ciążył na nim ciężar dowodowy z uwagi na podstawę prawną wezwania, a pomimo zasady jawności, ta doznaje ograniczenia na gruncie informacji gospodarczych stanowiących jego tajemnicę. Z tego też względu Zamawiający nie był w stanie nie tylko ustalić, skąd dane będą pobierane (o ile w ogóle, biorąc pod uwagę „bazę" udostępnioną w ramach próbki – por. pkt. 64 i 65), ale w kontekście badania realności ceny – czy koszt dostępu do baz danych został w ogóle przewidziany i uwzględniony w cenie oferty.

III.Zarzut dotyczący naruszenia art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) i 2) Ustawy polegający na zaniechaniu odrzucenia oferty wykonawcy TK-MED Sp. z o.o., a także zarzut naruszenia art. 239 ust. 1 i 2 Ustawy poprzez wybór oferty najkorzystniejszej.

86.Tytułem wstępu Zamawiający pragnie przypomnieć wymogi określone w punktach 11 oraz 145 lit. e i f opisu przedmiotu zamówienia: *System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX(…). Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając intuicyjność (25%), zgodność (75%). Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.*

87.Odwołujący podnosi, że „zgodnie z treścią Opisu przedmiotu zamówienia system musi spełniać powyższe wymagania. A contrario, literalne znaczenie słowa „musi" oznacza, że oferowany system nie może nie posiadać którejkolwiek z wymaganych funkcjonalności. (…) Jak wykazał Odwołujący, system oferowany przez TK-MED Sp. z o.o. nie posiada powyższych funkcjonalności w zakresie składni URI, co sam stwierdził Zamawiający podczas dokonanej oceny próbki." (str. 6 i 44 odwołania).

88.Z argumentacją Odwołującego nie sposób się zgodzić w świetle przywołanych postanowień opisu przedmiotu zamówienia, a dalej Zamawiający wykaże, że zarzut jest oczywiście bezzasadny.

89.Otóż zarzut opiera się na błędnej interpretacji sposobu weryfikacji wymagań stawianych systemowi. Zamawiający w pkt. 145 opisu przedmiotu zamówienia wprost zdefiniował autonomiczną dla tego postępowania definicję „spełnienia wymagania". W przeciwieństwie do typowej oceny spełnienia warunków (spełnia/nie spełnia), Zamawiający wprowadził względem próbki skalę procentową, gdzie próg akceptacji (uznania wymagania za spełnione) ustalono na poziomie 75%.

90.Jak wynika z protokołu oceny, oferta Wykonawcy TK-MED sp. z o.o. w zakresie wymagania nr 11 uzyskała wynik 92%. Oznacza to, że pomimo braku obsługi jednej z wymaganych składni (URI), stopień zgodności systemu z wymaganiem nr 11 (obejmującym również obsługę CEF, LEEF, XML, JSON, SYSLOG, REGEX oraz interfejs graficzn znacząco przekroczył minimalny próg określony w opisie przedmiotu zamówienia. Zgodnie z treścią pkt. 145, uzyskanie oceny powyżej 75% skutkuje uznaniem wymagania za spełnione. Odwołujący, kwestionując ten mechanizm na etapie oceny ofert, przedstawił zarzut, który należy uznać za spóźniony.

91.W świetle pkt. 145 opisu przedmiotu zamówienia, brak obsługi jednej ze składni (URI) przy jednoczesnym spełnieniu pozostałych składni, ale też samej możliwości parsowania logów i wsparcie dalszej normalizacji, skutkował jedynie obniżeniem oceny zgodności, ale nie mógł stać się podstawa do odrzucenia oferty. Wynik 92% (powyżej progu 75%) oznacza, że zgodnie z przyjętą w SWZ metodologią oceny oferta TK-MED sp. z o.o. spełnia omawiane wymaganie. Argumentacja Odwołującego stanowi jedynie próbę polemiki z zasadami oceny ofert, która nie zasługuje na uwzględnienie.

92.W świetle dotychczasowej argumentacji, Zamawiający wykazał również niezasadność zarzutu nr 4.

93.W oparciu o argumentację dot. spóźnionego zarzutu na postanowienia SWZ (por. pkt 90), zarzuty nr 5 i 6 również należy uznać za spóźnione, bo dotyczą sposobu oceny ofert. Abstrahując od przekroczenia terminu na zaskarżenie treści SWZ, Zamawiający zwraca uwagę, że na etapie postępowania począwszy od publikacji do dnia składania ofert, Odwołujący nawet nie podjął próby sygnalizacji rzekomej sprzeczności omawianych postanowień ani nie próbował wpłynąć na sposób zmiany ich treści. Stanowi to podstawę do stwierdzenia, że Odwołujący co najmniej godził się na taki sposób oceny wymagań, a dalej – oceny ofert, określony w SWZ. Próba ich podważania na obecnym etapie powinna zostać potraktowana jako niedopuszczalna próba przywrócenia terminu na zaskarżenie treści SWZ, a konsekwencji – odrzucenie. W razie innej kwalifikacji, zarzut winien podlegać oddaleniu jako bezzasadny.

Odwołujący w piśmie procesowym z 2.03. 2026 r. podał: (…) W odpowiedzi na prezentowane dotychczas stanowisko Zamawiającego oświadczam, że podtrzymuję twierdzenia zawarte w Odwołaniu i podnoszone na rozprawie w dniu 18 lutego 2026 r.

Jednocześnie wnoszę o przeprowadzenie dowodów z:
1)nagrań zawierających prezentację funkcjonalności systemu iS Sec- na fakt spełniania przez oferowany przez Odwołującego system wszystkich wymagań funkcjonalnych określonych przez Zamawiającego i brak wystąpienia przesłanek niezgodności treści oferty z warunkami zamówienia;
2)dokumenty zatytułowanego „SecureVisio Opracowanie"- na fakt nieprzedstawienia przez Przystępującego scenariusza testowania zaoferowanego przez niego systemu i dokonania przez Zamawiającego dowolnej oceny, stojącej w sprzeczności z zebranym w sprawie materiałem;
3)referencji wystawionych przez Gminy: Cieszanów, Horyniec Zdrój, Pacanów, Solec Zdrój i Przedsiębiorstwo Komunalne Gminy Radymno - na fakt intuicyjności oferowanego przez Odwołującego systemu i spełniania przez ten system wymagań stawianych tego typu systemom przez podmioty publiczne.

Odwołujący w pierwszej kolejności kwestionuje, aby oferowane oprogramowanie było programem Elastic Security jak insynuuje to Zamawiający. Z uwagi na skomplikowany charakter sprawy ocenianej przez Izbę, działania Zamawiającego zmierzają do rozmycia ocenianych kwestii i wprowadzenia Izby w błąd.

Moduł EDR, który znajduje się w systemie Odwołującego ma możliwość integracjiz modułami EDR oprogramowań różnych producentów, które zostały uwzględnione w instrukcji (tj. np. OpenEDR, WithSecure, ESET, Elastic Defend i innych). Jeżeli klient posiada, którykolwiek z modułów wskazanych w nawiasie (rozwiązania płatne), to wówczas w systemie IS SEC zostaje uruchomiony (widoczny) odpowiedni ,,podmoduł". Wskazane w Rozdziale 3 rozwiązania takie jak WithSecure, ESET czy właśnie Elastic Defend są rozwiązaniami komercyjnymi zewnętrznych dostawców. Złożona przez Odwołującego oferta nie obejmowała dostawy licencji ww. produktów. Wskazane w instrukcji obsługi zewnętrzne systemy nie są elementem oferowanego systemu IS SEC, tylko wskazują możliwość ich integracji, co z perspektywy Zamawiającego jest wartością dodaną.

Odwołujący wskazuje również, że nagrania, które Zamawiający dołączył jako dowody zostały wykonane już po ocenie naszej próbki - 02.12.2025, czyli po spotkaniu on-line z Odwołującym. Filmy te pokazują tylko jak Zamawiający zaniechał prawidłowej oceny systemu, zwłaszcza w kontekście rzekomego scenariusza testowania systemu TK-Med, o czym dalej.

Pkt 37 odpowiedzi na odwołanie Zamawiający pisze:
„Odnosząc się do twierdzenia Odwołującego odnośnie modułów UEBA oraz wskaźnika kompromitacji IoC i „niechęci sprawdzenia (przeklikania systemu) oraz brak wiedzy na jego temat oraz tego typu technologii i systemów uniemożliwił Zamawiającemu odnalezienie tych funkcjonalności", należy wskazać, że Odwołujący nie pokazał na żadnym zrzucie ekranu (a wcześniej w próbce) modułów zarządzania IoC ani UEBA. Instrukcja obsługi zawierała rozdział „Reguły korelacyjne", który nie zawierał żadnej treści– poniżej fragment instrukcji dostarczonej przez Odwołującego"

Analiza filmu potwierdza, że Zamawiający wybrał zakres dat ale nie zatwierdził tych dat jako sposobu filtrowania. Wybrane daty po prostu nie zostały zastosowane, co całkowicie wypaczyło wynik testu.

Dodatkowo Zamawiający w pkt 45 odpowiedzi wskazuje na rzekomą wadliwość rozwiązania systemu Odwołującego, który „wymaga ręcznego przepisania 32znakowego unikalnego identyfikatora zdarzenia nadrzędnego i przypisanie do zdarzenia podrzędnym (bądź incydentu podrzędnego do nadrzędnego)." Zamawiający przyznał na rozprawie, że nie "próbował" kopiować tylko przepisywał 32 bitowy ciąg znaków. Funkcja kopiuj/wklej używają wszyscy użytkownicy systemów. Zwłaszcza informatycy. To kolejny dowód na stosowanie przez Zamawiającego „podwójnych standardów oceny".

Zamawiający podnosił również na rozprawie, że scenariusz testowania Odwołującego nie pozwolił na odnalezienie określonych funkcjonalności systemu. Tymczasem Zamawiający wprowadził w błąd Izbę co do posiadania scenariusza testowania systemu TK-Med. W rzeczywistości dokument przekazany przez TK-Med nie jest scenariuszem testowania a jedynie opisem funkcjonalności. Zdumienie zatem budzi fakt, że system Odwołującego został oceniony negatywnie z uwagi na rzekomą niejednoznaczną instrukcję testowania, gdzie system TK-Med mimo braku obligatoryjnego scenariusza testowego został przez Zamawiającego zaakceptowany. To tylko pokazuje, że działaniom Zamawiającemu nie można przypisać jakiejkolwiek rzetelności.

Odwołujący składa również z niniejszym pismem nagrania prezentujące system iS Sec, które potwierdzają jednoznacznie, że posiada on wszelkie wymagania określone przez Zamawiającego. Poniżej objaśnienia poszczególnych filmów:

Punkt 1

IS Sec to system o budowie modułowej (posiada 15 modułów) wykorzystującym indeksową bazę danych Elastic Search do agregacji dużej ilości logów. System synchronizuje się dostępnymi darmowymi/komercyjnymi bazami danych zawierającymi istotne informację na temat podatności (CVE), wskaźników kompromitacji IOC, technik i taktyk działania cyberprzestępców (Matryca Mitre ATT&CK).
W opcji ustawienia – zakładka „zaawansowane" widać konsolę administracyjną Elastic wraz z linkiem Elastic Search nie

Elastic Security.

Punkt 2

System ISSec umożliwia tworzenierejestrów spełniających wymogi RODO art. 30. W module inwentaryzacji znajdują się zakładki oceny ryzyka z pokazanymi kategoriami danych. W zakładce „RODO" znajduje się raport , który możemy dostosować pod względem wyboru kolumn, a następnie eksportować w wybranym formacie. Zasoby widoczne w raporcie RODO dodajemy w module inwentaryzacji zaznaczając opcję "zasób przetwarzający dane osobowe", wypełniając rejestr przetwarzania danych osobowych dla wybranego zasobu, definiując szacowaną wartość sprzętu i oprogramowania, oraz danych i przechowywanych aktywów. Raporty naruszania danych osobowych generujemy w module SLA, w zakładce zagrożenia. Opcja ta jest widoczna po kliknięciu przycisku akcji dla wybranej pozycji.

Punkt 4

Interfejs graficzny ISSec pozwala na intuicyjne zarządzanie zdarzeniami oraz konfigurację akcji SIEM bezpośrednio z modułu monitoringu. Akcje oraz skrypty widoczne są po wybraniu odpowiadającej im zakładki. Użytkownik ma możliwość tworzenia własnych akcji po kliknięciu przycisku "Utwórz akcję". System automatycznie uruchamia ochronę na podstawie harmonogramu oraz reguł korelacyjnych (własnych i MITRE), wykorzystując przy tym algorytmy ML i reguły UEBA do wykrywania nietypowych zachowań. W module wykrywania zagrożeń, w zakładce matryca MITRE ATT&CK widoczny jest aktualny zakres taktyk i technik w oparciu o dostępne reguły. Dzięki scenariuszom SOAR, po wykryciu incydentu poza godzinami pracy, system może samoczynnie zablokować ruch sieciowy lub natychmiast powiadomić administratora. Tak owe playbooki tworzymy w module SOAR, w zakładce playbooki wybierając interesujący nas wyzwalacz, skrypty, akcje z możliwością dodania warunku. "Kafelki" na planszy playbooka możemy dowolnie ustawiać dzięki wsparciu funkcji "Drag and Drop", a połączenia pomiędzy nimi dodajemy po wciśnięciu przycisku w prawym górnym rogu planszy.

Punkt 11

IS Sec posiada moduł analizy logów który umożliwia wyświetlanie i wyszukiwanie wstępnie sprasowanych/ niesparowanych logów z różnych źródeł. W zakładce „indeksy" użytkownik może utworzyć własny indeks oraz w szczegółach indeksu skopiować/podglądnąć dostęp do niego przez udostępnione API. W zakładce „niestandardowe logi" użytkownik może wskazać lokalizację źródła logów poprzez podanie ścieżki do pliku/plików na wybranym hoście , oraz przypisanie ich do utworzonego wcześniej indeksu. Możliwość tworzenia parserów znajduję się w zakładce „parsery" co szczegółowo pokazuje film (parsery własne i predefiniowane). Film pokazuje również dodawanie indeksu oraz obsługiwane formaty danych. Zakładka „zawansowane wyszukiwanie" umożliwia filtrowanie poprzez dostępne źródła.

Punkt 23

Moduł monitoringu zasobów umożliwia przeglądniecie mapy sieci (mapa fizyczna) oraz pozwala na generowanie mapy logicznej. W zakładce tej istnieje możliwość zdefiniowanie parametrów na mapie. Kolorami zaznaczone są strefy bezpieczeństwa, a intuicyjnymi ikonami i strzałkami urządzenia oraz połączenia między nimi. Użytkownik po kliknięciu w wybrane urządzanie może podglądnąć do jakiej strefy został przypisany oraz dodawać/edytować dowolne parametry. Mapy możemy powiększać/pomniejszać, są skalowalne i dostosowują się do wszystkich urządzeń co widzimy na przedstawionym filmiku.

Punkt 40

Moduł analizy podatności automatycznie sprawdza wszystkie urządzenia oraz ich oprogramowanie zinwentaryzowane w systemie. Użytkownik z poziomu systemu może oznaczyć podatność jako rozwiązaną (zaakceptowaną). Po aktualizacji lub usunięciu oprogramowania wykryta wcześniej w systemie podatność zostanie automatycznie usunięta. System ISSec umożliwia integracje z skanerami podatności udostępniającymi API.

Punkt 51

Moduł wykrywania zagrożeń umożliwia tworzenie własnych reguł korelacyjnych. Zakładka „matrycy MITRE ATT&CK" pokazuje aktualny zakres taktyk i technik. W zakładce „reguły korelacyjne" użytkownik ma możliwość zmienić status reguły (włączyć/wyłączyć). Opcja „dodaj regułę" daje użytkownikowi możliwość tworzenia własnych reguł , dodawania taktyk, podtechnik. W module SOAR znajduje się zakładka „Playbooki" w której użytkownik może dodać własny playbook , wybrać wyzwalacz, technikę ATT&CK oraz regułę korelacyjną.

Punkt 72

Moduł SLA oraz moduł uprawnień umożliwia przypisanie operatorów do konkretnych grup incydentów oraz do rozwiązania wybranego incydentu. W zakładce „zagrożenia" użytkownik ma możliwość zaznaczenia interesującego go statusu i zastosować odpowiedni filtr. Użytkownik ma możliwość przypisania powiązanego zdarzenia, przypisać operatora który będzie odpowiedzialny za obsługę zdarzenia. W opcji ustawienia mamy możliwość edytowania/usuwania użytkowników , tworzyć/ edytować / usuwać grupy uprawnień. Zakładka ustawienia SLA umożliwia konfigurację, ustawienia limitów powiadomień, konfigurację reguł powiadomienia.

Punkt 75

W module SLA znajduje się zakładka „zdarzenia” gdzie grupowanie zdarzeń odbywa się poprzez wybranie opcji „przypisz zdarzenie” i podanie identyfikatora zdarzenia podrzędnego. Przy każdym zdarzeniu użytkownik ma możliwość wyświetlenia zagrożenia, przypisania zdarzenia, przypisania operatora oraz zareagowania.

Punkt 77

W module SLA w zakładce „zagrożenia” użytkownik wybiera - zdarzenia obsłużone. Po zastosowaniu filtru mamy możliwość wyświetlić historię obsługi danego zdarzenia.

Punkt 87

W module SLA w zakładce „podatności” użytkownik może wybrać odpowiednie akcje, oraz rozwinąć szczegóły danego zdarzenia. System wyposażony jest w zaawansowaną wyszukiwarkę umożliwiającą wyszukiwanie po kategorii oraz podanej frazy.

Punkt 96

W module UEBA znajdują się listy reguł EBA i UBA, rodzaj reguł wybieramy za pomocą przełącznika. W liście widoczna jest nazwa reguł, algorytm, współczynnik ryzyka, priorytet, status detektora oraz status reguły. Klikając przycisk „akcji” przy wybranej regule możemy wybrać opcję Detektor AI, gdzie mamy możliwość dostosowania parametrów detektora wybranej reguły, zmienić algorytm oraz przetrenować model AI.

Punkt 122

W module inwentaryzacji w zakładce „agenci” są widoczni wszyscy zainstalowani agenci oraz ich status dostępności. Są oni również widoczni, gdy przechodzimy do widoku urządzeń. Możemy monitorować statusy agentów oraz zdalnie nimi zarządzać. W module SOAR agenci realizują akcje z playbooków. Skrypty wykonywane przez agentów wybieramy z listy rozwijanej. Po kliknięciu w interesujący nas skrypt, jego “kafelek” pojawi się na planszy playbooka.

Punkt 125

W module Threat Intelligence widoczna jest lista potencjalnych zagrożeń oraz wskaźników kompromitacji dla wybranej za pomocą przełącznika kategorii danych: malware, zagrożenia sieciowe, złośliwe adresy URL. Na liście znajdziemy takie informacje jak: czas zdarzenia, wskaźnik wykrycia, sygnatura, rozmiar pliku, typ pliku i hash. Dla kategorii danych „malware” mamy możliwość podglądnąć szczegóły dla wybranej przez nas pozycji z listy oraz zablokować plik. Dla zagrożeń sieciowych i złośliwych adresów URL możemy również zobaczyć szczegóły oraz wyświetlić dodatkową informację. W zakładce Lista blokowanych plików, jak sama nazwa wskazuje możemy zobaczyć tak ową listę z możliwością edycji zablokowanego pliku lub usunięcia go z listy. Mamy możliwość wyeksportowania tych list w wybranych formacie.

Jak widać z powyższych opisów i udostępnionych materiałów wideo, które odnoszą się do poszczególnych punktów oceny dokonanej przez Zamawiającego, system iS Sec posiada wymagania przewidziane przez Zamawiającego. Jak niejednokrotnie Odwołujący podnosił, stwierdzenie niezgodności treści oferty z warunkami zamówienia wymaga udowodnienia, a nie jedynie domniemania, że niezgodność taka zachodzi. Zamawiający ciężarowi dowodu nie sprostał dokonując odrzucenia w oparciu o okoliczności nieustalone. Wysoka jakość systemu iS Sec została także wielokrotnie potwierdzona przez podmioty publiczne, które doceniają nie tylko poziom bezpieczeństwa, ale również intuicyjność, w którą Zamawiający tak uderza.

Mając na uwadze powyższe, Odwołujący podtrzymuje w pełni prezentowane dotychczas stanowisko i wnioskuje o uwzględnienie odwołania w całości, a w przypadku oddalenia zarzutów głównych, uwzględnienie zarzutu ewentualnego. Z uwagi na fragmentaryczną wypowiedź Zamawiającego zaprezentowaną na rozprawie w dniu 18 lutego 2026 r. Odwołujący zastrzega sobie prawo podnoszenia dalszych twierdzeń i przedstawiania dowodów.

Zamawiający w piśmie procesowym z dnia 10.03.2026 r. podał: (…) przedstawiam odpowiedź Zamawiającego na stanowisko zaprezentowane przez Odwołującego w piśmie z dnia 2 marca 2026 r.

1.Negacja Odwołującego zmierzająca do stwierdzenia, że oferowany system nie jest programem Elastic Security, a dostępny moduł EDR służy wyłącznie do integracji z modułami EDR innych producentów, Zamawiający odsyła do pkt. 13-17 niniejszego pisma.

2.Odwołujący twierdzi, że nagrania dołączone przez Zamawiającego jako dowody zostały wykonane po dacie oceny próbki, co ma jego zdaniem dyskredytować ich wartość. Ponadto ponownie zarzuca Zamawiającemu brak wiedzy technicznej i pominięcie zatwierdzenia dat w opcjach filtrowania zdarzeń, co rzekomo wypaczyło wynik testu. Odwołujący zarzuca również Zamawiającego nierzetelną ocenę dokumentacji i scenariuszy testowania systemu konkurencyjnego.

3.Po pierwsze, argument dotyczący daty wykonania nagrań nie ma wpływu na rozpoznanie sprawy i nie ma znaczenia z punktu widzenia oceny merytorycznej. Nagrania próbki systemu stanowią jedynie udokumentowanie czynności Zamawiającego, które ten zrealizował na udostępnionym środowisku testowym. W dniu utrwalenia wideo próbka znajdowała się w stanie tożsamym z dniem samej oceny.

4.Po drugie, zarzut rzekomego "niezatwierdzenia dat do filtrowania" należy oceniać w oparciu o dostarczoną przez

Odwołującego dokumentację, która stanowiła podstawę badania zgodnie z pkt. 144 opisu przedmiotu zamówienia. Odwołujący stara się zestawić własne scenariusze testowania z dokumentacją Przystępującego, jednak milczy nt. faktycznej jakość instrukcji obsługi obu systemów.

5.System oferowany przez Przystępującego posiada obszerną instrukcję obsługi, która po wyeksportowaniu do formatu pdf na domyślnych ustawieniach liczy 2076 stron formatu A4, rozłożonych w 178 rozdziałach. Jest to objętość ponad 5-krotnie większa niż w przypadku systemu ISSec.

6.Instrukcja systemu SecureVisio Przystępującego zawiera szczegółowy słownik wykorzystywanych wyrażeń, wykaz wszystkich modułów i sposobów komunikacji. Dla przykładu same reguły korelacyjne są tam opisane na 20 stronach, dodatkowo zawierają stronę opisu ze zrzutami ekranu jak weryfikować funkcjonalność. Opis nazw zmiennych stosowanych m.in. w regułach korelacyjnych, to kolejne 4 strony instrukcji, z merytorycznymi odniesieniami do innych rozdziałów.

7.Z drugiej strony leży dokumentacja systemu ISSec, która jest pełna błędów i skupia się na objaśnianiu zagadnień błahych z punktu widzenia przeznaczenia systemu (np. wielokrotne tłumaczenie i pokazywanie, czym różni się zaznaczony checkbox od niezaznaczonego). Jako instrukcję weryfikacji zaawansowanych funkcjonalności, takich jak reguły korelacyjne czy zarządzanie modułami (IoC, UEBA), Zamawiający otrzymał od Odwołującego polecenie sprowadzające się do zdania: „Przeglądnij dostępne opcje”.

8.Działania Zamawiającego widoczne na nagraniu, w tym to, w jaki sposób nawigował po interfejsie i korzystał (lub nie) z filtrów, były bezpośrednim wynikiem jakości dokumentacji Odwołującego, która nie zawierała konkretnych wytycznych technicznych. Ocena badanej próbki zawsze uwzględnia całość dokumentacji dostarczonej przez wykonawców.

9.Właśnie z powodu omówionych braków w dokumentacji, kierując się dyspozycją pkt. 145 opisu przedmiotu zamówienia, Zamawiający doprowadził do spotkania on-line z Odwołującym. Celem tego spotkania było odniesienie się do wyników oceny zgodności systemu, które przekazano Odwołującemu z wyprzedzeniem. Dało to Odwołującemu możliwość przygotowania się i prezentacji tych funkcjonalności, których Zamawiający nie był w stanie samodzielnie zlokalizować na podstawie instrukcji.

10.Niemniej w toku spotkania Odwołujący ograniczył się wyłącznie do gołosłownych twierdzeń i pustych zapewnień, że „system spełnia wymogi OPZ”. Nie poparł tego żadnym dowodem w postaci demonstracji działania systemu na dostarczonej próbce, uchylając się od zapewnienia wsparcia technicznego. Na ponawiane przez Zamawiającego pytania dotyczące konkretnego sposobu wywołania nieodnalezionych funkcjonalności, Odwołujący nie był w stanie udzielić ani jednej merytorycznej odpowiedzi, która dawałaby podstawy do rewizji dotychczasowej oceny.

11.Co więcej, Zamawiający wykazał się dobrą wolą, proponując dołączenie do spotkania innych osób po stronie Odwołującego, które faktycznie znają system, a nawet zadeklarował możliwość przedłużenia spotkania na kolejny dzień roboczy. Odwołujący propozycję odrzucił, godząc się tym samym z dotychczasową oceną systemu. Takie zachowanie Odwołującego: bierność, brak dowodów oraz odmowa współpracy, Zamawiający uznał za brak odpowiedzi na ujawnione braki, a w konsekwencji uznanie, że zaoferowany system nie spełnia wymagań mu postawionych.

12.W kolejnych punktach Zamawiający prezentuje stanowisko będące odpowiedzią na dostarczony materiał wideo wraz z opisem przez Odwołującego.

Punkt 1 opisu przedmiotu zamówienia

13.Odwołujący, opierając się na nowo przedłożonym nagraniu wideo (plik Punkt 1).mp4), twierdzi, że jego system posiada budowę modułową i wykorzystuje jedynie "indeksową bazę danych Elastic Search". Na dowód wskazuje, że w zakładce "zaawansowane" widnieje link z nazwą "Elastic Search", a nie "Elastic Security", co ma rzekomo dowodzić, że system nie korzysta z zakazanej platformy, a jedynie z samego silnika bazy danych.

14.Przedstawiony przez Odwołującego dowód z nagrania wideo nie tylko nie potwierdza jego tezy, ale stanowi dowód na to, że oferowany system korzysta z Elastic Security. Twierdzenie, że nazwa widniejąca w adresie ("Elastic Search") w interfejsie graficznym, konfigurowanym przez Odwołującego, jest dowodem na rodzaj użytej technologii w tle, jest swoistym testem wiedzy, czy adresat nagrania (tu: Izba) ma wiedzę o zasadzie działania subdomen i konfiguracji adresu URL, stanowiącego bezpośredni do nich dostęp. Tekst linku czy nazwa subdomeny to zmienne, które twórca nakładki graficznej może dowolnie modyfikować. Nie stanowi to dowodu co do architektury systemu.

15.Adres URL wskazany przez Odwołującego na nagraniu wideo nie stanowi żadnego dowodu na rodzaj zastosowanej technologii, a jego prezentacja jest manipulacją. Odwołujący, próbując udowodnić, że jego system korzysta jedynie z bazy danych, wskazuje na nagraniu link prowadzący do adresu „elasticsearch.infosoftware.pl”. Taki argument stanowi próbę wprowadzenia Izby w błąd, z uwagi na mechanizmy działania sieci Internet:

1)Adres „infosoftware.pl” jest domeną firmową należącą do Odwołującego. Zgodnie z architekturą systemu DNS, właściciel domeny głównej ma swobodę w tworzeniu tzw. subdomen. Administrator sieci Odwołującego skonfigurował subdomenę o nazwie elasticsearch.infosoftware.pl równie swobodnie, co mógł uczynić stosując np. „baza-danych.infosoftware.pl”. Nazwa ta jest wyłącznie ciągiem znaków wpisanym przez samego Odwołującego na potrzeby

środowiska testowego. Zbieżność nazwy subdomeny z nazwą silnika bazy danych nie jest dowodem na to, co jest zainstalowane, a jedynie deklaracją Odwołującego wpisaną w konfigurację serwera DNS.
2)Zamawiający jedynie zaznacza, że Odwołujący mógł skonfigurować przekierowanie http/https, co powoduje udostępnienie pod danym adresem URL dowolnej usługi działającej w tle, niezależnie od jej faktycznej nazwy widniejącej w pasku adresu. Oznacza to, że administrator Odwołującego mógł zainstalować i uruchomić interfejs Kibana (wchodzący w skład darmowego SIEM Elastic Security), a następnie regułą sieciową przekierować na niego ruch sieciowy z adresu „elasticsearch.infosoftware.pl". Użytkownik klikający w taki link zobaczy w pasku przeglądarki rzekomy "elasticsearch", podczas gdy będzie korzystał z interfejsu Kibany.
16.Zamawiający zwraca uwagę na fragment nagrania od 03:42 do 03:48 (plik Punkt 1).mp4), w którym w prawym dolnym rogu pojawia się komunikat „in a production environment, it is recommended that you configure server.publicbaseurl". Treść ostrzeżenia dotyczy niezgodnej z rekomendacjami konfiguracji parametru server.publicBaseURL. Zmienna server.publicBaseURL nie jest parametrem silnika bazy danych Elasticsearch. Jest to parametr konfiguracyjny (znajdujący się w pliku kibana.yml) dla narzędzia Kibana – będącego interfejsem graficznym i silnikiem systemu Elastic. Kibana to moduł odpowiedzialny za wizualizację, analizę logów, zarządzanie alertami i regułami SIEM.
17.Zgodnie z oficjalną dokumentacją producenta, baza Elasticsearch nie posiada wbudowanych graficznych narzędzi analitycznych, wizualizacyjnych ani interfejsu do zarządzania alertami SIEM. Wszystkie te funkcje są realizowane przez aplikację Kibana. Zatem ujawniony błąd parametru server.publicBaseUrl na nagraniu dostarczonym przez Odwołującego, stanowi dowód na obecność Kibany w systemie Odwołującego. Odwołujący nie ograniczył się wyłącznie do samej bazy danych, ale wdrożył zestaw oferowanych aplikacji, tworzących darmowy system SIEM.
Punkt 11 opisu przedmiotu zamówienia
18.Odwołujący twierdzi, że system posiada wymagany moduł do wyświetlania i wyszukiwania logów. Wskazuje, że zakładki „indeksy", „niestandardowe logi" oraz „zawansowane wyszukiwanie" pozwalają na zarządzanie logami, natomiast załączony film ma stanowić dowód, że w zakładce „parsery" znajduje się możliwość tworzenia parserów oraz obsługi wspieranych formatów danych.
19.Tytułem przypomnienia Zamawiający ponowie przywoła treść wymogu: „System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX.".
20.Jak wykazano na nagraniu (plik Punkt 11).mp4), w obrębie całego udostępnionego materiału, system prezentuje się odmiennie niż sugeruje to narracja Odwołującego. Wymieniane przez niego zakładki „indeksy" czy „niestandardowe logi" dotyczą ścieżek dostępu i miejsca danych w systemie, co pozostaje irrelewantne dla przywołanego wymagania (spór wszakże dotyczy parsowania, a nie miejsca położenia logów w systemie).
21.Należy jednak zwrócić uwagę na zakładkę „parsery". Otóż prezentowany na nagraniu proces w rzeczywistości stanowi parsowanie REGEX (wyrażenia regularne, liniowe). Na materiale wideo w żadnym momencie nie zaprezentowano dedykowanego graficznego interfejsu (GUI) dla formatów ustrukturyzowanych, hierarchicznych takich jak XML czy JSON. Odwołujący w dalszym ciągu nie udowadnia istnienia opcji typu „wybierz z listy format XML", lecz na nagraniu prezentuje ogólne pole edytora tekstu, które wymusza na operatorze ręczne wpisanie wyrażeń regularnych (REGEX), służących do liniowego przeszukiwania tekstu. Zastosowanie mechanizmu REGEX do wszystkich wymienionych w opisie przedmiotu składni świadczy o braku dedykowanych narzędzi w systemie, co było przedmiotem omówienia w odpowiedzi na odwołanie.
22.Zamawiający odniesie się również do fragmentu omawianego nagrania w momencie 2:05 pliku Punkt 11).mp4. Odwołujący w tym miejscu nagrania najeżdża kursorem na ikonę informacji (tzw. tooltip), co wywołuje podpowiedź tekstową: „Obsługiwane formaty danych: JSON, XML, LEEF, CEF, Syslog (RFC 3164), Syslog (RFC 5424)". Sam fa wymienienia w tym tekście obsługiwanych formatów nie może stanowić dowodu na spełnienie omawianego wymagania. Wyświetlona podpowiedź tekstowa jest wyłącznie statycznym tekstem informacyjnym (plikiem pomocy dla operatora). Wymaganie nie dotyczyło jednak wyświetlenia słów kluczowych w dokumentacji czy tekstach pomocy, lecz posiadania gotowego interfejsu graficznego (GUI) służącego do tworzenia reguł normalizacji dla określonych formatów. Informacja "Dodaj dane do indeksu" umieszczona nad polem do wprowadzania kodu oznacza jedynie, że w tym polu operator może spróbować napisać wyrażenie regularne, które pobierze dane z formatu ustrukturyzowanego. Nadal nie jest to dedykowany parser graficzny, lecz jedynie podpowiedź, że w polu tekstowym można użyć wyrażeń regularnych.
Punkt 40 opisu przedmiotu zamówienia
23.Tytułem przypomnienia, Zamawiający wymagał, żeby „System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu".

24.Odwołujący twierdzi, że jego system iS Sec ma otwartą strukturę i integruje się z każdym dostępnym na rynku skanerem podatności za pomocą udostępnionego API. Brak zaprezentowania integracji z trzema skanerami Odwołujący tłumaczy kosztami zakupu licencji. Dodatkowo Odwołujący zarzuca Zamawiającemu nierówne traktowanie, twierdząc, że konkurencyjna oferta została oceniona pozytywnie, mimo że jej integracja była realizowana przez zewnętrzne skrypty „powershell", podczas gdy Odwołujący polega na wbudowanym API. W opisie własnego nagrania Odwołujący dodaje jedynie, że system umożliwia integrację ze skanerami udostępniającymi API.
25.W dostarczonym przez Odwołującego nagraniu mającym dowodzić spełnienie wymogów z pkt. 40, system nie wyświetla ani nie posiada graficznego interfejsu użytkownika (GUI) pozwalającego na konfigurację integracji z trzema zewnętrznymi skanerami podatności. Nagranie ukazuje jedynie wbudowany, własny skaner iS Sec. Wymóg opisu przedmiotu zamówienia wprost narzucał, że wszystkie operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu. API jest wyłącznie interfejsem programistycznym, a nie interfejsem graficznym. W udostępnionej instrukcji obsługi oraz w zaprezentowanej próbce brakuje jakiejkolwiek dokumentacji API, a system operuje wyłącznie względem wbudowanego skanera. W żaden sposób nie udowodniono, by operator był w stanie samodzielnie skonfigurować integrację ze skanerem. Twierdzenie Odwołującego, że to w ramach wdrożenia skonfiguruje system tak, żeby był w pełni zintegrowany, jest jednoznacznym przyznaniem, że oferowany system takiej gotowej, konfigurowalnej z poziomu GUI integracji nie posiada. Zapewnienia o możliwości "napisania" lub "połączenia" systemu w przyszłości za pomocą API nie spełniają wymogu Zamawiającego.
26.Próbka systemu w dniu badania nie posiadała wymaganej funkcjonalności, co potwierdza nowy materiał wideo. System nie dysponuje graficznym interfejsem do konfiguracji integracji z trzema zewnętrznymi skanerami podatności, a możliwość zaprogramowania takiej integracji przez producenta w przyszłości z użyciem API nie stanowi spełnienia wymogu postawionego w punkcie 40 opisu przedmiotu zamówienia.
Punkt 51 opisu przedmiotu zamówienia
27.Zgodnie z opisem przedmiotu zamówienia: „System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać: (...) c. atrybuty użytkowników z Active Directory, d. atrybuty komputerów z Active Directory, e. bazę wskaźników kompromitacji (IOC), f. informacje z elektronicznej dokumentacji, g. anomalie w zachowaniu użytkowników (UBA), h. anomalie w zachowaniu zasobów (EBA), i. podatności na zasobach, j. wyniki analizy konfiguracji".
28.Odwołujący podejmuje próbę udowodnienia spełnienia wymogu, powołując się na dostarczony materiał wideo. W opisie wskazuje, że moduł pozwala na tworzenie reguł, dodawanie taktyk i podtechnik z „matrycy MITRE ATT&CK" oraz że w module SOAR (w zakładce Playbooki) można dodać własny playbook i powiązać go z regułą korelacyjną. Odwołujący jednak pomija brak możliwości korelacji w oparciu o parametry wskazane w lit. c-j.
29.Jak wynika z nagrania dostarczonego w pliku Punkt 51).mp4, ale też wcześniej dostarczonym przez Zamawiającego pn. Reguły korelacyjne IS Sec.mp4, Odwołujący nie zaprezentował żadnego sposobu wykorzystania w regułach korelacyjnych danych wymaganych w lit. c, d, e, f, g, h, i oraz j punktu 51 opisu przedmiotu zamówienia.
30.Widoczne na nagraniu dodawanie taktyk MITRE ATT&CK realizuje wyłącznie wymóg z lit. k. Z kolei prezentacja modułu SOAR i playbooków jest bezprzedmiotowa – playbooki służą do automatyzacji reakcji na incydent, a opis przedmiot zamówienia wymagał, aby mechanizm uwzględniał wymienione atrybuty „na bieżąco na etapie rejestrowania danych w systemie".
31.Co więcej, odnośnie wymogu zdefiniowanego w lit. c pkt. 51 (atrybuty użytkowników z Active Directory), metoda wykorzystania tych danych zadeklarowana przez Odwołującego ex post podczas rozprawy, została poddana uprzedniej weryfikacji przez Zamawiającego. Wynik weryfikacji wykazał, że wskazana przez Odwołującego metoda jest niemożliwa do wykonania w dostarczonym systemie.
Punkt 122 opisu przedmiotu zamówienia
32.Zgodnie z pkt 122 lit. b-i, Zamawiający wymagał od oprogramowania agentowego m.in.: zbierania logów z plików tekstowych (b) i logów dotyczących zdarzeń innych niż standardowe (c), zdolności do monitorowania integralności plików (d), rejestru systemowego (e), urządzeń zewnętrznych (f), komunikacji szyfrowanej protokołem HTTPS (g), możliwości monitorowania stanu agentów w konsoli zarządzającej (h) oraz przygotowania różnych zestawów konfiguracji (i).
33.Odwołujący przedłożył nowy dowód w postaci materiału wideo wraz z opisem, w którym wskazuje, że agenci i ich status dostępności są widoczni w module inwentaryzacji (zakładka „agenci") oraz w widoku urządzeń. Ponadto twierdzi, że umożliwia to monitorowanie statusów agentów oraz zdalne zarządzanie nimi. Na koniec wskazuje, że agenci realizują akcje z playbooków SOAR za pomocą skryptów wybieranych z listy rozwijanej.
34.Niemniej materiał dowodowy Odwołującego nie odnosi się do istoty wcześniej opisanych braków. Odwołujący prezentuje wyłącznie moduł inwentaryzacji (widoczność agentów) oraz uruchamianie gotowych skryptów z modułu SOAR. Nie zaprezentowano żadnego dowodu na zdolność agenta do monitorowania rejestru, integralności plików czy

portów USB. Odwołujący nie przedstawił dowodu przeciwnego na stwierdzone Zamawiającego braki, podnoszone w odpowiedzi na odwołanie oraz podczas rozprawy. Przedłożone nagranie nie wnosi niczego nowego do rozpoznania istoty sprawy. Pominięcie spornych funkcji w demonstracji należy poczytywać jako przyznanie, że oferowany system nie posiada wymaganych funkcjonalności.

35.Co się tyczy "statusu dostępności" w widoku inwentaryzacji, to Zamawiający odwołuje się do pkt. 60 i n. odpowiedzi na odwołanie, zgodnie z którymi wyświetlany status odnosi się do ogólnej dostępności urządzenia w sieci, a nie do faktycznego stanu działania procesu agenta, czego wprost wymagał Zamawiający.

Pozostałe punkty opisu przedmiotu zamówienia: 40, 72, 75, 87, 125

36.W odniesieniu do twierdzeń sformułowanych przez Odwołującego w punktach 40, 72, 75, 87 oraz 125, Zamawiający wskazuje, że dostarczony w tym zakresie materiał wideo wraz z załączonym do niego opisem stanowią jedynie powielenie argumentacji prezentowanej już we wcześniejszych wystąpieniach Odwołującego.

37.Argumentację w w/w zakresie należy traktować wyłącznie jako polemikę. Przedłożone przez Odwołującego dowody nie wnoszą do sprawy nic nowego i nie prezentują żadnych nowych faktów. W związku z tym, że materiały te nie stanowią dowodu przeciwnego wobec poczynionych ustaleń z badania próbki systemu, tj. nie ujawniają funkcjonalności, których brak został uprzednio stwierdzony i opisany, nie zasługują na osobne omówienie. Dalsza polemika z twierdzeniami Odwołującego w tym zakresie jest bezprzedmiotowa z punktu widzenia oceny stanu faktycznego, wobec czego Zamawiający jedynie odsyła w tym zakresie do stanowiska zaprezentowanego w odpowiedzi na odwołanie.

Skład Orzekający Krajowej Izby Odwoławczej (Izba lub KIO) ustalił i zważył, co następuje:

Odwołanie nie podlega uwzględnieniu.

Odwołujący, InfoSoftware Polska Sp. z o.o. z/s w Szczepańcowej (wykonawca InfoSoftware) kwestionuje w odwołaniu odrzucenie oferty wykonawcy podnosząc zarzut naruszenia (1) art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) - 3) ustawy Pzp, oraz (2) art. 226 ust. 1 pkt 8) w zw. z art. 224 ust. 6 ustawy Pzp i wskazując na bezzasadne odrzucenie oferty Odwołującego jako (a) niezgodnej z warunkami zamówienia, gdy w rzeczywistości oferowany system spełnia wszystkie wymagania określone przez Zamawiającego w OPZ, a ocena intuicyjności rozwiązań jest sprzeczna z ustawą i nieproporcjonalna do zaspokojenia uzasadnionych potrzeb Zamawiającego, oraz (b) błędne uznanie, że cena oferty Odwołującego jest rażąco niska i niezaakceptowanie wyjaśnień złożonych przez Odwołującego, gdy wyjaśnienia te potwierdzają, że cena nie jest rażąco niska. Także Odwołujący kwestionuje wybór najkorzystniejszej oferty Uczestnika TK-Med., podnosząc zarzut naruszenia: (1) art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) i 2) ustawy Pzp oraz art. 239 ust. 1 i 2 ustawy Pzp i wskazując na (a) zaniechanie odrzucenia oferty TK-MED Sp. z o.o., gdy zaoferowany przez tego wykonawcę system nie posiada wymaganych opisem przedmiotu zamówienia funkcjonalności, oraz (b) wybór oferty tego wykonawcy, która najkorzystniejsza nie jest.

Odwołujący wskazuje także na zarzuty ewentualne na wypadek nieuwzględnienia powyższych zarzutów przez Izbę, a mianowicie wykonawca podniósł zarzut naruszenia: (1) art. 239 ust. 1 i 2 ustawy Pzp z uwagi na wybór oferty w sytuacji, w której postępowanie podlega unieważnieniu, oraz (2) art. 255 pkt 6) w zw. z art. 457 ust. 1 pkt 1) w zw. z art. 99 ust. 1 i 4 i w zw. z art. 16 pkt 1) i 2) ustawy Pzp ustawy Pzp, z uwagi (…) *na zaniechanie unieważnienia postepowania w sytuacji, gdy postępowanie to obarczone jest niemożliwą do usunięcia wadą, która powoduje niemożność zawarcia niepodlegającej unieważnieniu umowy, wynikającą z wewnętrznie sprzecznego i niejednoznacznego opisu przedmiotu zamówienia, który nie pozwala na prawidłową ocenę ofert, jak również daje Zamawiającemu prawo subiektywnej oceny niezgodności systemu z jego oczekiwaniami przez pryzmat niezdefiniowanej intuicyjności*".

W decyzji z 17.12.2025 r. Zamawiający odnośnie oferty wykonawcy InfoSoftware podał: (…) *Zamawiający informuje o odrzuceniu oferty wykonawcy InfoSoftware Polska spółka z ograniczoną odpowiedzialnością z siedzibą w Szczepańcowej (dalej „Wykonawca") na podstawie art. 226 ust. 1 pkt 5 ustawy oraz art. 226 ust. 1 pkt 8 ustawy*". W uzasadnieniu Zamawiający przedstawiając okoliczności dla zastosowania wskazanych przesłanek miał na uwadze informacje zastrzeżone przez wykonawcę jako tajemnica przedsiębiorstwa i wynikające z tych zastrzeżeń ograniczenia. Pierwsze zastrzeżenie wynika z pisma z 14.11.

2025 r., które dotyczyło informacji – jak podał wykonawca – zawartych w (…) *Próbce oferowanego systemu, instrukcji i protokole z jej badania (…) będące integralną częścią oferty* (…). Podobne zastrzeżenie zamieścił w piśmie z 9.12.2026 r., które stanowiło wyjaśnienia w odpowiedzi na wezwanie zamawiającego w przedmiocie oferowanej ceny.

Izba kierując się również ograniczeniami wynikającymi z zastrzeżonych informacji jako tajemnica przedsiębiorstwa przez Odwołującego w wyjaśnieniach z 9.12.2025 r. (niekwestionowanymi przez Zamawiającego i oferentów) wskazuje za Zamawiającym na okoliczności podane w uzasadnieniu decyzji z 17.12. 2025 r. (…)

- w punkcie II.1 (…)

W przedmiotowym Postępowaniu Zamawiający wymagał, aby oferowany system przeciwdziałający cyberzagrożeniom, umożliwiający ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi, spełniał wymagania określone w opisie przedmiotu zamówienia. W szczególności Zamawiający

zwraca uwagę na następujące wymagania względem systemu (poszczególne punkty odzwierciedlają numerację punktów w opisie przedmiotu zamówienia):
1) Zamawiający nie dopuszcza rozwiązań z otwartym kodem źródłowym ani rozwiązań darmowych, w tym rozwiązań posiadających płatne opcje wsparcia z darmowym oprogramowaniem jak np. Elastic Security, AlienVault, Wazuh, OSSIM, Snort itp.
11) System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG REGEX. System musi umożliwiać zastosowanie wszystkich typów składni dla pojedynczego zdarzenia, przykładowo pole „msg" znormalizowane automatycznie według standardu CEF powinno mieć możliwość dalszej normalizacji np.: zgodnej z URI lub REGEX. 40) System musi zawierać mechanizm integracji ze skanerami podatności co najmniej trzech producentów. W ramach integracji system musi mieć możliwość uruchamiania skanowania podatności, importowania jego wyników zawierających listę podatności i ich atrybuty oraz możliwość kasowania ze skanera zaimportowanych wcześniej skanów. Wszystkie powyższe operacje muszą być konfigurowalne z poziomu graficznego interfejsu systemu.
51) System musi posiadać interfejs graficzny do tworzenie własnych reguł korelacyjnych odpowiedzialnych za wykrywanie określonych zdarzeń pojawiających się w systemie. Korelacja musi odbywać się na bieżąco na etapie rejestrowania danych w systemie a mechanizm tworzenie reguł musi uwzględniać:
a.sparsowane pola oraz ich wartości,
b.listy referencyjne,
c.atrybuty użytkowników z Active Directory,
d.atrybuty komputerów z Active Directory,
e.bazę wskaźników kompromitacji (IOC),
f.informacje z elektronicznej dokumentacji,
g.anomalie w zachowaniu użytkowników (UBA),
h.anomalie w zachowaniu zasobów (EBA),
i.podatności na zasobach,
j.wyniki analizy konfiguracji,
k.techniki MITRE ATT&CK®,
72) System powinien mieć logikę automatycznego przypisywania zdarzeń zakwalifikowanych do obsługi wraz z powiadomieniem operatora, któremu zostało ono przydzielone (min. e-mail, SMS). Kwalifikacja musi uwzględniać m.in. dostępność operatora, jego obciążenia oraz parametry zasobu, którego dotyczy zdarzenie, typ zasobu (np.: serwer lub stacja robocza), jego krytyczność oraz realizowane z jego udziałem usługi z katalogu usług. Na przykład: zdarzenie przypisane do krytycznego serwera realizującego usługę DNS powinny trafić do innego operatora niż zdarzenia dotyczące pozostałych serwerów usług sieciowych.
87) Obsługiwane w systemie podatności muszą być dostępne w formie listy umożliwiającej ich filtrowanie po następujących wartościach:
a.wyliczonym priorytecie podatności,
b.aktualnym statusie obsługi,
c.ważności zasobu, na którym została wykryta,
d.adresie IP tego systemu,
e.parametrów SLA związanych z tym statusem,
f.przetwarzanych na zasobach informacji, np.: lista podatności dotycząca tylko systemów przetwarzających dane osobowe,
g.parametrach CVSS, np.: lista podatności których „Access Complexity (AC)" = „low" oraz „Access Vector (AV) = „Network".
122) Rozwiązanie SIEM musi wspierać obsługę aplikacji typu agent na systemy Windows (Windows Agent), które posiadają nie mniej niż następujące możliwości:
a.centralne zarządzanie i możliwość aktualizacji z głównej konsoli zarządzającej;
b.możliwość zbierania logów z plików tekstowych na urządzeniach z zainstalowanym systemem z rodziny Windows;
c.możliwość zbierania logów dotyczących zdarzeń rodzajów innych niż: Security,
System, Application;
d.zdolność do monitorowania integralności plików;
e.zdolność do monitorowania rejestru systemowego;
f.zdolność do monitorowania urządzeń zewnętrznych (removable devices);
g.agent instalowany na systemach z rodziny Windows musi komunikować się z poszczególnymi komponentami rozwiązania SIEM w sposób zaszyfrowany z wykorzystaniem protokołu HTTPS;

h.musi istnieć możliwość monitorowania stanu agentów w konsoli zarządzającej systemu;
i.musi istnieć możliwość przygotowania różnych zestawów konfiguracji agenta, a następnie przypisywania ich niezależnie do dowolnej ilości (jeden lub więcej) systemów źródłowych. Np. inne konfiguracje dla kontrolerów domeny, a inne dla serwerów DNS;
j.musi umożliwiać automatyzację reakcji na zagrożenie, jak blokowanie zdefiniowanego ruchu sieciowego czy blokada procesu.
125) System musi być zintegrowany z zewnętrznymi bazami o zagrożeniach (Threat Inteligence Feeds - TI) oraz zawierać już zintegrowany zestaw niekomercyjnych (open source) lub komercyjnych baz zagrożeń.
Wykonawca w złożonej ofercie, w ramach systemu SIEM, zaoferował program iS SEC SIEM, którego jest producentem.
Zamawiający, kierując się punktem 144 opisu przedmiotu zamówienia, wymagał, by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający, w czasie dwóch dni roboczych, zweryfikował zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w opisie przedmiotu zamówienia. Zamawiający zastrzegł jednocześnie, że w przypadku stwierdzenia niezgodności próbki i dokumentacji z wymaganiami opisu przedmiotu zamówienia, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta zostanie odrzucona. W przypadku gdy Wykonawca nie dołączyłby do oferty próbki systemu wraz z dokumentacją, oferta również zostałaby odrzucona.
W świetle punktu 145 opisu przedmiotu zamówienia, Wykonawca był zobowiązany umożliwić weryfikację Zamawiającemu na dostarczonej próbce systemu wybranych wymagań opisu przedmiotu zamówienia, co do których Zamawiający nie uzyskał wystarczających informacji potwierdzających ich zgodność. Rozwiązanie miało być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami opisu przedmiotu zamówienia oraz pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, Wykonawca miał obowiązek przygotowania odpowiedniej instrukcji oraz zapewnić wsparcie konsultanta technicznego. Procedura weryfikacji spełnienia wymagań opisu przedmiotu zamówienia miała przebiegać następująco:
a.Zamawiający dokona wyboru min. 10 wymagań opisu przedmiotu zamówienia, które zostaną zaprezentowane przez Wykonawcę na systemie demonstracyjnym;
b.Wykonawca w terminie 2 dni od wyboru wymagań dostarczy zwięzły opis do każdego z wybranych wymagań, określający zakres planowanych testów demonstracyjnych;
c.Wykonawca w terminie 3 dni od dostarczenia opisu dokona przygotowania systemu demonstracyjnego, w tym: dokona odpowiedniej konfiguracji systemu
(umożliwiającegoweryfikację wskazanych wymagań opisu przedmiotu zamówienia), przygotuje instrukcję dostępową do systemu demonstracyjnego; opracuje instrukcję realizacji zaproponowanych scenariuszy testowania;
d.Wykonawca przekaże Zamawiającemu dostęp do systemu demonstracyjnego na okres 3 dni w celu analizy zgodności z opisem przedmiotu zamówienia oraz weryfikacji intuicyjności obsługi.
e.Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając intuicyjność (25%) oraz zgodność (75%).
f.Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.
Wykonawca w okresie 3 dni od otrzymania oceny ze strony Zamawiającego miał możliwość wyznaczenia spotkania w formie zdalnej, podczas którego mógł odnieść się do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. W razie braku organizacji spotkania lub nieprzedstawienia odpowiedzi na ocenę Zamawiającego, Zamawiający uzna, że oferowane rozwiązanie nie spełnia wymagań opisu przedmiotu zamówienia.
Kierując się powyżej przywołanymi wymaganiami, Zamawiający pismem z dnia 18 listopada 2025 r. wezwał Wykonawcę do dostarczenia zwięzłego opisu do każdego z wybranych przez Zamawiającego wymagań, tj. wymagań obligatoryjnych w następujących punktach opisu przedmiotu zamówienia: 1, 11, 23, 40, 51, 72, 75, 77, 87, 96, 122, 125, a także wymagań opcjonalnych wskazanych w punktach 2 i 4, określający zakres planowanych testów demonstracyjnych.
W wyznaczonym terminie Wykonawca przekazał opis wymagań i przekazał dostęp do systemu demonstracyjnego. W wyniku oceny wymagań, Zamawiający stwierdził i przekazał Wykonawcy informację o następujących wadach systemu:

Fragment ukryty stanowi tajemnicę przedsiębiorstwa.

Następnie, kierując się brzmieniem punktu 145 opisu przedmiotu zamówienia, Zamawiający w dniu 2 grudnia 2025 r. uczestniczył w spotkaniu z Wykonawcą celem umożliwienia odniesienia się do wyników oceny zgodności i intuicyjności systemu. Wykonawca po pierwsze nie zaprezentował kwestionowanych funkcjonalności, a jedynie poinformował, że oferta i oferowany system spełniają wymagania zakreślone treścią opisu przedmiotu zamówienia, po czym zaproponował kolejny termin spotkania na dzień 8 grudnia 2025 r.

Kierując się zasadą równego traktowania wykonawców, Zamawiający odmówił Wykonawcy drugiego spotkania i stwierdził w świetle powyższej oceny, że system oferowany przez Wykonawcę uzyskał wynik badania na poziomie 52%, co kwalifikuje go jako wynik negatywny:

Fragment ukryty stanowi tajemnicę przedsiębiorstwa.

Tym samym oferta Wykonawcy podlega odrzuceniu jako niezgoda z warunkami zamówienia na podstawie art. 226 ust. 1 pkt 5 ustawy".

II.2

- w punkcie II.2 (…)

Zamawiający, działając na podstawie art. 224 ust. 1 ustawy, wezwał Wykonawcę do złożenia wyjaśnień, w tym złożenie dowodów, w zakresie wyliczenia ceny oferty, w celu weryfikacji możliwości wykonania przedmiotu zamówienia zgodnie z wymaganiami określonymi w dokumentach zamówienia lub wynikającymi z odrębnych przepisów.

Jednocześnie Zamawiający zakreślił następujący szczegółowy obszar, podlegający wyjaśnieniu:

Fragment ukryty stanowi tajemnicę przedsiębiorstwa.

Mając na uwadze powyższe, należy stwierdzić, że Wykonawca nie obalił domniemania rażąco niskiej ceny. Złożone wyjaśnienia potwierdziły, że cena oferty wynika z pominięcia w/w elementów wymagających wyceny, takie jak choćby płatne wsparcie licencyjne, których brak zagraża należytemu wykonaniu umowy. Zgodnie z art. 224 ust. 6 ustawy odrzuceniu jako oferta z rażąco niską ceną lub kosztem podlega oferta wykonawcy, jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadniają podanej w ofercie ceny lub kosztu.

Mając na uwadze powyższe, Zamawiający odrzuca ofertę Wykonawcy na podstawie art. 226 ust. 1 pkt 8 ustawy".

Odwołujący w zakresie pierwszej z podstaw odrzucenia oferty wykonawcy (art. 226 ust. 1 pkt 5 ustawy Pzp) przede wszystkim w odwołaniu podał, że Zamawiający nie zdefiniował w żaden sposób co i w jaki sposób (w oparciu o jakie kryteria) będzie oceniał pod kątem „intuicyjności". Także stwierdził, że Zamawiający w sposób niejasny i sprzeczny z pozostałą treścią Opisu przedmiotu zamówienia opisał zasady oceny „Zgodności". Zdaniem wykonawcy, zgodnie z tym opisem, system może nie posiadać funkcjonalności, co do których Zamawiający napisał wcześniej, że posiadać je musi.

Przede wszystkim w związku z ograniczeniami wynikającymi z art. 515 ust.2 pkt 2 ustawy Pzp za spóźnione należy uznać kwestionowanie opisu zasad oceny wskazanych m.in. w punkcie 145 lit. e. Jak słusznie zauważał Zamawiający, nastąpiło przekroczenia terminu na zaskarżenie treści SWZ, wykonawca nie podjął, począwszy od publikacji do dnia składania ofert, próby sygnalizacji rzekomej sprzeczności wskazanych w odwołaniu postanowień ani nie domagał się zmiany ich treści z zastosowaniem dostępnych środków ochrony prawnej. Zatem wykonawca, co najmniej godził się na taki sposób oceny wymagań, na etapie oceny próbki i w konsekwencji oceny ofert, określony w OPZ i SWZ. Uwzględnienie argumentacji odwołania w tym zakresie powodowałoby niedopuszczalną próbę przywrócenia terminu na zaskarżenie tych postanowień OPZ - SWZ. Tym samym zarzut w takim aspekcie podnoszony nie podlegał rozpoznaniu, co w konsekwencji stanowi odpowiednio o oddaleniu zarzutu w tym zakresie.

Mając natomiast na uwadze zarzut, co do jego meritum podnoszony wobec oceny przez Zamawiającego spornych parametrów, Izba miała na uwadze następujące postanowienia dokumentacji i wskazywane przez Strony i Uczestnika TK-MED okoliczności:

W Specyfikacji Warunków Zamówienia (SWZ) w punkcie IV.1 wskazano, że *„Przedmiotem zamówienia jest zakup, dostarczenie i wdrożenie w środowisku informatycznym Zamawiającego systemu przeciwdziałającemu cyberzagrożeniom, umożliwiającego ich wykrywanie przy wsparciu mechanizmów uczenia maszynowego oraz zapewniającego automatyzację i orkiestrację ich obsługi*" . Z kolei w punkcie IV.5 podano: *„5. Szczegółowy opis oraz sposób realizacji zamówienia zawiera Opis Przedmiotu Zamówienia (OPZ), stanowiący Załącznik nr 8 do SWZ".*

W OPZ wskazano jakie wymagania powinien spełniać oferowany System.W tym dokumencie – mając na uwadze kwestie sporne - w punktach 144) i 145) wskazano:

144)*Zmawiający wymaga by wraz ofertą Wykonawca dostarczył próbkę systemu (np. w postaci przekierowania do wersji demonstracyjnej systemu) z odpowiednią dokumentacją (np. w postaci karty produktu oraz niezbędnych instrukcji). Zamawiający maksymalnie w ciągu dwóch dni roboczych, zweryfikuje zgodność oferowanego systemu na podstawie próbki systemu i dostarczonej dokumentacji, porównując je ze wszystkimi wymaganiami określonymi w powyższych punktach OPZ. W przypadku gdy Zamawiający uzna niezgodność próbki i dokumentacji z wymaganiami OPZ, lub gdy Zamawiający nie odnajdzie określonego wymagania w próbce systemu i dokumentacji, oferta Wykonawcy zostanie odrzucona. W przypadku gdy Wykonawca nie dołączy do oferty próbki systemu wraz z dokumentacją, oferta zostanie odrzucona*.

145)*Wykonawca musi umożliwić weryfikację przez Zamawiającego na dostarczonej próbce systemu wybranych wymagań OPZ, co do których Zamawiający nie uzyskał wystarczających informacji potwierdzających ich zgodność. Rozwiązanie musi być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami OPZ oraz pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, Wykonawca musi przygotować odpowiednią instrukcję oraz zapewnić*

wsparcie konsultanta technicznego. Procedura weryfikacji spełnienia wymagań OPZ będzie przebiegać następująco:
a.Zamawiający dokona wyboru min. 10 wymagań OPZ, które zostaną zaprezentowane przez
Wykonawcę na systemie demonstracyjnym;
b.Wykonawca w terminie 2 dni od wyboru wymagań OPZ (ppkt. a) dostarczy zwięzły opis do każdego z wybranych wymagań, określający zakres planowanych testów demonstracyjnych;
c.Wykonawca w terminie 3 dni od dostarczenia opisu (ppkt b) dokona przygotowania systemu demonstracyjnego, w tym: dokona odpowiedniej konfiguracji systemu (umożliwiającego weryfikację wskazanych wymagań OPZ), przygotuje instrukcję dostępową do systemu demonstracyjnego; opracuje instrukcję realizacji zaproponowanych scenariuszy testowania;
d.Wykonawca przekaże Zamawiającemu dostęp do systemu demonstracyjnego na okres 3 dni w celu analizy zgodności z OPZ oraz weryfikacji intuicyjności obsługi.
e.Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając:
-Intuicyjność (25%)
-Zgodność (75%)
f.Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.
g.Wykonawca w okresie 3 dni od otrzymania oceny ze strony Zamawiającego (ppkt. f) ma możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego odniesie się on do wyników oceny zgodności i intuicyjności systemu, opracowanych przez Zamawiającego. Jeśli w wyznaczonym terminie Wykonawca nie zorganizuje spotkania i/lub nie przedstawi odpowiedzi na ocenę Zamawiającego zostanie uznane, że oferowane rozwiązanie spełnia wymagań OPZ.
Dodatkowe wymagania, które będą oceniane jako spełnia/nie spełnia, których oferowany program nie musi posiadać, ale będą one dodatkowo oceniane:
1)Skaner podatności. Zamawiający dostarczy odpowiednią licencję na skaner podatności, na czas nieograniczony. Dopuszczalne jest rozwiązanie posiadające odpłatne aktualizacje pod warunkiem, że oferowana licencja zawiera darmowe dla zamawiającego aktualizacje na okres identyczny jak okres wsparcia pakietu oprogramowania.
2)System umożliwia stworzenie kompletnych w zasoby informacji rejestrów spełniających wymogi art. 30 RODO m. in. rejestru czynności oraz rejestru kategorii czynności przetwarzania zawierających informacje dotyczące przede wszystkim:
a.celu/kategorii przetwarzania
b.związku z procesem,
c.określenia kategorii danych wraz z kategorią osób, których dane są przetwarzane
d.oznaczenia podstawy prawnej oraz wymaganej zgody na przetwarzanie danych e. określenia źródła danych
f.informacją na temat retencji danych / planowanego terminu usunięcia
g.wskazania systemów i oprogramowania do przetwarzania danych wraz z określeniem ich zabezpieczeń
h.określenia zastosowanych środków bezpieczeństwa - organizacyjnych i technicznych i wielu innych istotnych z punktu widzenia właściwej ochrony dla przetwarzanych danych osobowych.
System powinien dodatkowo:
a.Usprawniać proces inwentaryzacji obszarów przetwarzania danych osobowych poprzez wyszukiwanie systemów IT przetwarzających tego typu dane jak również grup i kategorii danych osobowych.
b.System wyznacza dostępne zabezpieczenia techniczne w odniesieniu do potencjalnych źródeł zagrożenia dla systemów IT przetwarzających dane osobowe.
c.System automatycznie wykonuje analizę ryzyka danych osobowych w odniesieniu do zagrożeń natury informatycznej oraz wykonuje ocenę skutków dla ochrony danych dla trzech głównych ryzyk: ryzyka utraty poufności, integralności oraz dostępności danych osobowych.
d.System wykonuje analizę ryzyka dla przetwarzanych danych osobowych wraz z określeniem zarówno zagrożeń jak i konsekwencji na jakie narażone są osoby fizyczne z związku z przetwarzaniem ich danych osobowych.
e.System umożliwia szacowanie ryzyka od momentu wdrażania organizacyjnych i technicznych środków bezpieczeństwa przez cały proces przetwarzania danych osobowych w organizacji. Cały proces monitorowania poziomu zagrożeń oraz zapewniania rozliczalności w odniesieniu do zastosowanych zabezpieczeń jest więc procesem ciągłym i na bieżąco dostrajanym.
f.System zapewnia spełnienie wymagań formalno-prawnych dotyczących raportowania naruszeń bezpieczeństwa danych osobowych zgodnie z art. 33 pkt 5 RODO umożliwiając w pełni automatyczne generowanie „Raportu naruszenia ochrony danych osobowych dla organu nadzorczego" łącznie z wyznaczeniem możliwych konsekwencji naruszenia

bezpieczeństwa.

g.System automatyzuje wykonywanie oceny skutków dla ochrony danych osobowych wraz z automatycznym generowaniem raportów w obszarze analizy ryzyka cyberzagrożeń (art. 35 RODO).

h.System pozwala na przechowywanie dokumentów dotyczących systemu ochrony danych osobowych umożliwiając użytkownikom śledzenie zmian w dokumentach, informowanie o zmianach oraz pełnym nadzorem nad dostępem do dokumentów. (…)

Izba, uwzględniając wskazane postanowienia OPZ zgodziła się z Zamawiającym, że wymagana wraz z odpowiednią dokumentacją próbka w formie dostępu demonstracyjnego pełniła funkcję dowodową celem potwierdzenia, że oferowany system spełnia wymagania określone w OPZ. Zadaniem takiej próbki – stanowiącej integralną część oferty na co wskazywał sam Odwołujący w piśmie z 14.11.2025 r. - było potwierdzenie, że oferowany dany System działa w sposób wymagany w OPZ. W świetle tych postanowień wymagana próbka nie mogła być postrzegana jako ilustracja możliwości wykonawcy i jego wizji systemu. Miała bowiem pokazać konkretne rozwiązania Systemu w kontekście wymaganych, ich istnienie, a nie wytworzenie na etapie realizacji zamówienia oraz potwierdzić spełnianie określonych funkcjonalności przez System i wykluczyć te niedopuszczone OPZ jak w pkt 1. Zgodnie z tym pkt 1 Zamawiający nie dopuścił (…) *rozwiązań z otwartym kodem źródłowym, ani rozwiązań darmowych, w tym rozwiązań posiadających płatne opcje wsparcia z darmowym oprogramowaniem jak np. Elastic Security, AlienVault, Wazuh, OSSIM, Snort itp.*".

Izba zgodziła się również z Zamawiającym, że ta próbka stanowiła element oferty. Miała bowiem referować do konkretnego rozwiązania, które wykonawca oferuje i którą to próbką ma wykazać spełnianie wymagań i ich zgodności z SWZ, w tym przypadku z OPZ stanowiącym integralną część SpecyfikacjiW ramach wymienionych punktów wskazano na procedurę oceny próbki. W ramach tej procedury wykonawca miał umożliwić Zamawiającemu weryfikację na dostarczonej próbce systemu wybranych wymagań OPZ, co do których Zamawiający nie uzyskał w ramach samodzielnej oceny wystarczających informacji potwierdzających ich zgodność. Rozwiązanie miało być skonfigurowane w sposób umożliwiający jego weryfikację z wymaganiami OPZ oraz pozwalać na zdalny dostęp. W ramach dostępu do rozwiązania, wykonawca miał przygotować odpowiednią instrukcję oraz zapewnić wsparcie konsultanta technicznego. Procedura weryfikacji spełnienia wymagań OPZ także wynika z tego punktu, a mianowicie w określonych terminach miało nastąpić:

wybór min. 10 wymagań OPZ, które zostaną zaprezentowane przez wykonawcę na systemie demonstracyjnym – zadanie zamawiającego;

dostarczenie zwięzłego opisu do każdego z wybranych wymagań, określający zakres planowanych testów demonstracyjnych – zadanie wykonawcy;

przygotowanie systemu demonstracyjnego, w tym: dokonanie odpowiedniej konfiguracji systemu (umożliwiającego weryfikację wskazanych wymagań OPZ), przygotowanie instrukcji dostępowej do systemu demonstracyjnego; opracowanie instrukcji realizacji zaproponowanych scenariuszy testowania – zadanie wykonawcy;

przekazanie dostępu do systemu demonstracyjnego - zadanie wykonawcy;

analiza zgodności z OPZ oraz weryfikacji intuicyjności obsługi i ocena każdego z 10 wybranych wymagań, uwzględniając kryteria: (-) Intuicyjność (25%) oraz (-) Zgodność (75%) - zadanie Zamawiającego

Izba zgodziła się z Zamawiającym, że w OPZ – w opisie sposobu oceny próbki -jednoznacznie podano, że w przypadku, gdy próbka nie zawiera pewnych funkcji wymaganych względem niej i później całego systemu, przyjmuje się, że oferowany system ich nie posiada. Próbkę należało zatem traktować jako wycinek możliwości produktu wykonawcy w momencie składania ofert. Zamawiający w oparciu o wybrany wycinek (10 wymagań) badając wybrane wymagania oceniał System jako całość. To badanie następowało w oparciu o przygotowane scenariusze testowe. Izba zwraca też uwagę, że wynik tej oceny nie był arbitralny. Wykonawca bowiem po otrzymaniu oceny Zamawiającego (ppkt f) miał możliwość wyznaczenia spotkania w formie zdalnej (np. za pomocą platformy: Teams, Zoom lub Webex), podczas którego miał możliwość odniesienia się do wyników oceny zgodności i intuicyjności systemu. Zamawiający w postępowaniu dowodowym przed Izbą wskazał na spotkanie 2 grudnia 2025 r., podając (jak w decyzji z 17.12.2025 r.), że w toku spotkania wykonawca zapewniając, że „system spełnia wymogi OPZ", nie poparł tego twierdzenia żadnym dowodem w postaci prezentacji działania systemu, a na pytania dotyczące sposobu wywołania nieodnalezionych funkcjonalności nie udzielił odpowiedzi, które pozwoliłyby na zmianę dotychczasowej oceny. Tak jak podkreślał Zamawiający, w trakcie rozprawy, a czego Odwołujący nie obalił przeciwnym dowodem, wykonawca nie zapewnił wymaganego w pkt 145 wsparcia technicznego. Także wykonawca nie zakwestionował przed Izbą, że negatywnie odniósł się do propozycji Zamawiającego dotyczącej dołączenia do spotkania w tym dniu innych osób znających system oraz przedłużenia spotkania na kolejny dzień roboczy. Tym samym godził się z dotychczasową oceną, że zaoferowany System nie spełnia wymagań określonych w opisie przedmiotu zamówienia. Przedłożone do pisma procesowego z 2.03.2026 r. filmy nie mogły być uznane za dowód na potwierdzenie, że ustalenia Zamawiające na spotkaniu 2 grudnia 2025 r. były nieprawidłowe. Przede wszystkim stosowne wyjaśnienia na fakt spełniania przez oferowany przez

Odwołującego system wszystkich wymagań funkcjonalnych określonych przez Zamawiającego i brak wystąpienia przesłanek niezgodności treści oferty z warunkami zamówienia powinny być przedłożone na spotkaniu w dniu 2 grudnia 2025 r. lub na przedłużonym spotkaniu, o którym mowa w punkcie 77 pisma Zamawiającego z 6.02.
2026 r. W tym punkcie, co nie zostało podważone na rozprawie, Zamawiający odwołał się do jego propozycji ze spotkania 2.12.2025 r. która dotyczyła dołączenia do spotkania innych osób znających system a także deklarowanego przedłużenia spotkania na kolejny dzień roboczy. Izba ponadto zgodziła się z Zamawiającym, że argument dotyczący daty wykonania nagrań przedłożonych do odpowiedzi z 6.02. 2026 r. nie ma znaczenia z punktu widzenia oceny merytorycznej próbki Odwołującego. Te nagrania stanowią bowiem tylko udokumentowanie czynności Zamawiającego, które ten zrealizował na udostępnionym przez wykonawcę środowisku testowym. Dotyczą próbki systemu w stanie tożsamym - co nie zostało podważone przez wykonawcę w toku rozprawy - z dnia oceny tej próbki. Z kolei wskazane wcześniej Odwołującego - jak argumentował Zamawiający - nie stanowią dowodu przeciwnego wobec ustaleń Zamawiającego z badania próbki systemu, a mianowicie nie ujawniają funkcjonalności, których brak stwierdził Zamawiający w piśmie z 18.11. 2025 r. Te dowody nawiązują bowiem do argumentacji wykonawcy prezentowanej w odwołaniu i pismach procesowych.

Reasumując, Izba uznała, że Odwołujący przygotowując próbkę nie postępował w zgodności z wymaganiami OPZ, w tym co do prezentacji próbki Systemu w ramach procedury jej oceny.Zważywszy na zastrzeżone informacje zawarte w próbce oferowanego systemu, instrukcji i protokole z jej badania (wg pisma z 14.11.2025 r.) Izba kierując się informacjami zawartymi w odwołaniu (jawnym) oraz w odpowiedzi na odwołanie (jawnej) i pismach procesowych w zakresie wyznaczonym ich granicami zwraca uwagę na następujące kwestie wskazujące na brak podstaw kwestionowania oceny Zamawiającego przedstawionej w decyzji z 17.12. 2025 r. Mając na uwadze przebieg i wynik spotkania 2.12.2025 r., które odnosiło się do spornych wymagań i/lub funkcjonalności, argumentacja Odwołującego nie jest kompatybilna z wymaganiami OPZ. Podobnie stanowisko w odwołaniu jak i w piśmie procesowym dowodzi, że Odwołujący przygotowując próbkę nie postępował w zgodności z wymaganiami OPZ co do funkcjonalności jak i co do prezentacji próbki, w tym uczestnictwa wykonawcy w ramach procedury jej oceny. Odwołujący na spotkaniu 2.12.2025 r. miał odnieść się przy wsparciu konsultanta technicznego wykonawcy do zdiagnozowanych przez Zamawiającego wad systemu. W przekazanej informacji Zamawiający wskazał na postanowienia OPZ i jego ustalenia w oparciu informacje, które uzyskał na podstawie pisma, które skierował do wykonawcy 18 11. 2025 r. Tym pismem bowiem wezwał wykonawcę do dostarczenia zwięzłego opisu do każdego z wybranych wymagań obligatoryjnych w punktach OPZ: 1, 11, 23, 40, 51, 72, 75, 77, 87, 96, 122, 125, a także wymagań opcjonalnych wskazanych w punktach 2 i 4, określający zakres planowanych testów demonstracyjnych. W wyniku oceny wymagań stwierdził, a następnie przekazał wykonawcy informację o wadach systemu w podanych punktach. Jak już wskazano na spotkaniu 2.12.2025 r. wykonawca oprócz zapewnień co do zgodności Systemu z OPZ nie wykazał tych funkcjonalności, których dotyczyło pismo z 18.11.2026 r. Wymaga podkreślenia, że w świetle postanowień OPZ (w tym pkt 144) ciężar dowodowy spełniania wymagań spoczywał na Odwołującym, który był zobowiązany do wykazania, że oferowany system IT spełnia wymagania Zamawiającego. W ramach procedury wyjaśnień - w procedurze zdalnej - to wykonawca miał wykazać, że wbrew pierwotnej ocenie Zamawiającego, oferowany system spełnia wymagania. Ze stanu faktycznego tej sprawy wynika, że w dniu 2.12.2025 r. wykonawca nie wykazał, że ustalenia Zamawiającego co do wskazanych wad sytemu w piśmie z 18.11.2025 r. są nieprawidłowe. Wymaga podkreślenia, że Krajowa Izba Odwoławcza rozpoznając – jak w tym stanie faktycznym - zarzut naruszenia art. 226 ust.1 pkt 5 Pzp ustala, czy odrzucając ofertę wykonawcy w konkretnej dacie Zamawiający naruszył przepisy ustawy Pzp i/lub postanowienia SWZ (OPZ). Ze stanu faktycznego tej sprawy wynika, że podstawą decyzji Zamawiającego z 17.12.2025 r. był wynik ustaleń sfinalizowanych spotkaniem 2.12.2025 r. w ramach procedury opisanej w OPZ w odniesieniu do próbki oferowanego systemu i dokumentacji przedłożonej do tego systemu, na którym to spotkaniu ustalenia Zamawiającego według pisma z 18.11.2025 r. nie zostały skutecznie podważone.

Tym samym podnoszony w odwołaniu zarzut odrzucenia oferty Odwołującego z naruszeniem art. 226 ust.1 pkt 5 w zw. z art. 16 pkt 1) -3) podlega oddaleniu jako niezasadny.

W odwołaniu w zakresie drugiej z podstaw odrzucenia oferty wykonawcy (art. art. 226 ust. 1 pkt 8 ustawy Pzp) Izba zwraca uwagę na treść wezwania z 4.12.2025 r. w którym Zamawiający wskazując na art. 224 ust. 1 Pzp wezwał wykonawcę (…) do szczegółowego uzasadnienia i przedstawienia dowodów, w zakresie:
1.Metodologii i harmonogramu prac: Prosimy o szczegółowy opis planowanych etapów wdrożenia systemu SIEM/SOAR, w tym analizy, projektowania, konfiguracji, testów oraz przekazania do eksploatacji.
2.Zastosowanych rozwiązań technicznych/licencyjnych: Prosimy o wyjaśnienie, czy przyjęte założenia wpływają na obniżenie kosztów, bez uszczerbku dla jakości i funkcjonalności wymaganych w SWZ. W szczególności prosimy o wymienienie wszystkich licencji wykorzystywanego oprogramowania zawartego w końcowym produkcie, w tym oprogramowania open-source, producenta i w jaki sposób jest zapewnione dla niego wsparcie na okres wymagany w SWZ (pkt. 141 OPZ). Równocześnie prosimy o podanie z jakiego adresu i na jakiej licencji są pobierane wymagane w

OPZ dane do systemu.
3.Zasobów kadrowych: Prosimy o podanie liczby i kwalifikacji (certyfikaty, doświadczenie w projektach SIEM/SOAR) osób, które zostaną oddelegowane do realizacji zamówienia, wraz z uzasadnieniem ich efektywności i kosztów pracy.
4.Efektywność i oszczędności: Wszelkie inne obiektywne czynniki, które pozwoliły Państwu na skalkulowanie ceny na tak niskim poziomie (np. posiadane unikalne know-how, zautomatyzowane procesy).
5.Informację o ewentualnych ukrytych kosztach jak np. konieczność zakupu akceleratora do obsługi modelu AI wykorzystanego w systemie SIEM.
Jednocześnie przypominamy, iż zgodnie z art. 224 ust. 5 p.z.p. obowiązek wykazania, że oferta nie zawiera rażąco niskiej ceny spoczywa na Wykonawcy. Należy podkreślić, iż zgodnie z art. 224 ust. 6 p.z.p. Zamawiający odrzuci ofertę Wykonawcy, który nie udzielił wyjaśnień w wyznaczonym terminie lub jeżeli złożone wyjaśnienia wraz z dowodami nie uzasadnią podanej w ofercie ceny. Zamawiający oceniając złożone wyjaśnienia będzie brał pod uwagę również okoliczności, o których mowa w art. 224 ust. 3 p.z.p., w szczególności w zakresie:
-zgodności z przepisami dotyczącymi kosztów pracy, których wartość przyjęta do ustalenia ceny nie może być niższa od minimalnego wynagrodzenia za pracę albo minimalnej stawki godzinowej, ustalonych na podstawie przepisów ustawy z dnia 10 października 2002 r. o minimalnym wynagrodzeniu za pracę lub przepisów odrębnych właściwych dla spraw, z którymi związane jest realizowane zamówienie;
-zgodności z przepisami z zakresu prawa pracy i zabezpieczenia społecznego, obowiązującymi w miejscu, w którym realizowane jest zamówienie. (…)

Izba mając na uwadze wyjaśnienia z 9.12.2025 r. wykonawcy złożone w odpowiedzi na to konkretne wezwanie oraz uwzględniając fakt zastrzeżenia tych informacji jako tajemnica przedsiębiorstwa, wskazuje na okoliczności podnoszone przez Zamawiającego w odpowiedzi na odwołanie, które są zgodne z treścią złożonych wyjaśnień. Mianowicie wykonawca nie odniósł się do elementów, do których odnosi się wezwanie, o czym wykonawca został poinformowany w piśmie z 17.12. 2025 r. w jego punkcie II.2. Tak jak wskazywał Zamawiający w odpowiedzi na odwołanie i co potwierdza treść wyjaśnień, wykonawca InfoSoftware składając wyjaśnienia co do kosztów pracy posłużył się dowodem abstrakcyjny. Jako jedyny dowód na realność przyjętych stawek dla dwóch osób przedstawił bowiem zrzuty ekranu z portalu wynagrodzenia.pl. W tych wyjaśnieniach posłużył się także ogólnym sformułowaniem o posiadaniu „grona specjalistów", „zaangażowaniu zasobów kadrowych", nie precyzując informacji na ich temat, które pozwoliłyby na weryfikację kosztów. Słusznie podnosił Zamawiający, że stwierdzenie o „gronie specjalistów" nie jest nośnikiem jakiejkolwiek informacji o zatrudnianych faktycznie specjalistach o specjalnościach przydatnych do realizacji tego projektu i ich liczbie. Izba zwraca uwagę, że wykonawca zgodnie z wezwaniem miał odnieść się do jego zasobu kadrowego ze wskazaniem l*iczby* i *kwalifikacji (certyfikaty, doświadczenie w projektach SIEM/SOAR) osób, które zostaną oddelegowane do realizacji zamówienia, wraz z uzasadnieniem ich efektywności i kosztów pracy".* Izba zgodziła się z Zamawiającym, że brak wskazania konkretnej liczby osób i ich kwalifikacji uniemożliwiał Zamawiającemu ocenę, czy cena oferty jest realna. Ponadto powoływanie się na anonimowe „grono" bez pokrycia w liczbach i kosztach nie jest wykonaniem wezwania do złożenia wyjaśnień. Odwołujący ponadto w miejsce abstrakcyjnych dowodów miał praktyczną możliwość przedstawić przykładowo zanonimizowane umowy o pracę (lub inny rodzaj umów), raporty ZUS czy listy płac. Posłużenie się bowiem wydrukami internetowymi), wobec ciężaru dowodu, obrazowało tylko koszty jakie ponoszą statystyczni przedsiębiorcy, a nie dowodem realności ceny tego wykonawcy. Izba także zwraca uwagę, że zgodnie z treścią wezwania Zamawiający wymagał podania adresu i licencji, z których będą pobierane wymagane dane do systemu. W tym przypadku wykonawca w miejsce żądanych podał, że w zakresie baz danych, z którymi łączy się system, bazy te są ogólnie dostępne, ale ich podanie nie było wymagane w treści specyfikacji, a stanowi tajemnicę przedsiębiorstwa wykonawcy. Zatem, jak uznał słusznie Zamawiający, w oparciu o taką informację nie był w stanie ustalić choćby tego, „czy dostęp do baz danych jest bezpłatny, czy też wymaga poniesienia kosztu – a jeśli tak, to w jakiej wysokości". Także słusznie Zamawiający zwrócił uwagę, że na wykonawcy, który ubiega się o udzielenie zamówienia publicznego, z uwagi na podstawę prawną wezwania, spoczywa ciężar dowodowy, a zasada jawności, doznaje ograniczenia na gruncie informacji gospodarczych stanowiących jego tajemnicę, ale wobec konkurentów, a nie koniecznie – zdaniem Izby - wobec Zamawiającego, który jest zobowiązany zachować poufność takich informacji.

W konkluzji izba stwierdza, że wskazane okoliczności dowodzą, że wbrew twierdzeniu Odwołującego, wykonawca nie złożył obszernych wyjaśnień ze wskazaniem wszystkich istotnych kosztów, które w pełni potwierdzają, że zaoferowana cena pozwala na wykonanie zamówienia zgodnie z wymaganiami Zamawiającego. Tym samym podnoszony w odwołaniu zarzut odrzucenia oferty wykonawcy InfoSoftware z naruszeniem art. 226 ust. 1 pkt 8) w zw. z art. 224 ust. 6 ustawy Pzp nie podlega uwzględnieniu.

Odwołujący w odwołaniu odnośnie oferty TK-MED, wskazując na zaniechanie odrzucenia oferty tego wykonawcy stwierdził, że zaoferowany przez tego wykonawcę system nie posiada wymaganych opisem przedmiotu zamówienia funkcjonalności. Odniósł brak funkcjonalności do wymagania z punktu 11 OPZ.Tak jak wskazał Zamawiający powołując

się na protokół oceny, oferta TK-MED sp. z o.o. w zakresie wymagania 11 uzyskała wynik 92%.
Zgodnie z wymaganiem określonym w punktach 11 oraz 145 lit. e i f opisu przedmiotu zamówienia: *System musi być wyposażony w graficzny interfejs do tworzenia dodatkowych reguł normalizacji (parserów) dla zdarzeń z niestandardowych źródeł danych, w oparciu o następujące składnie: CEF, LEEF, URI, XML, JSON, SYSLOG, REGEX). Zamawiający oceni każde z 10 wybranych wymagań, uwzględniając intuicyjność (25%), zgodność (75%). Każde z wymagań może uzyskać maksymalną ocenę 100%. Wymaganie uznaje się za niespełnione, gdy jego ocena zostanie określona przez Zamawiającego poniżej poziomu 75%. Procentowa suma wszystkich wymagań nie może być niższa niż 90%.*
Wskazany zatem wynik w związku z cytowanym postanowieniem OPZ oznacza i co podkreślał Zamawiający, że pomimo braku obsługi jednej z wymaganych składni (URI), stopień zgodności systemu wykonawcy TK-MED z wymaganiem nr 11 (obejmującym również obsługę CEF, LEEF, XML, JSON, SYSLOG, REGEX oraz interfejs graficzn znacząco przekroczył minimalny próg określony w opisie przedmiotu zamówienia. Zgodnie ze wskazanym postanowieniem z pkt 145, próbka TK-MED uzyskała w pkt 11 ocenę powyżej 75%. Izba ponownie podkreśla, że Odwołujący na etapie oceny ofert, nie może skutecznie kwestionować mechanizmu oceny próbki. Zamawiający w pkt 145 OPZ – jak podnosił - zdefiniował autonomiczną dla tego postępowania definicję „spełnienia wymagania". W przeciwieństwie do typowej oceny spełnienia warunków (spełnia/nie spełnia), Zamawiający wprowadził względem próbki skalę procentową, gdzie próg akceptacji (uznania wymagania za spełnione) ustalono na poziomie 75%. W świetle pkt 145 opisu przedmiotu zamówienia, brak obsługi jednej ze składni (URI) przy jednoczesnym spełnieniu pozostałych składni i możliwości parsowania logów i wsparcie dalszej normalizacji, skutkował jedynie obniżeniem oceny zgodności, ale nie mógł stanowić podstawy do odrzucenia oferty.

W konkluzji izba stwierdza, że wynik 92% (powyżej progu 75%) - zgodnie z przyjętą w OPZ metodologią oceny uzyskany przez ofertę TK-MED w wymaganiu z pkt 11 potwierdza spełnianie tego wymagania. Tym samym podnoszony zarzut zaniechania odrzucenia oferty tego wykonawcy na podstawie art.226 ust.1 pkt 5 w zw. z art. 16 pkt 1) i 2) nie podlega uwzględnieniu.

W odniesieniu do zarzutu ewentualnego art. 255 pkt 6) w zw. z art. 457 ust. 1 pkt 1) w zw. z art. 99 ust. 1 i 4 i w zw. z art. 16 pkt 1) i 2) ustawy Pzp, Izba uznała ten zarzut za niezasadny. W zakresie tego zarzutu Odwołujący powołując się na przesłankę zgodnie z którą unieważnienie następuje wówczas (…) *gdy postępowanie to obarczone jest niemożliwą do usunięcia wadą, która powoduje niemożność zawarcia niepodlegającej unieważnieniu umowy (…)* wskazuje, że ta wada wynika z „*wewnętrznie sprzecznego i niejednoznacznego opisu przedmiotu zamówienia, który nie pozwala na prawidłową ocenę ofert, jak również daje Zamawiającemu prawo subiektywnej oceny niezgodności systemu z jego oczekiwaniami przez pryzmat niezdefiniowanej intuicyjności*".

Ta argumentacja dotyczy kwestionowanej zasady oceny próbek – sposobu oceny – która jak już wskazywano jest co do zasady spóźniona. Jak również wskazywano termin na zaskarżenie SWZ w tym jej załącznika – OPZ – jest przekroczony. Izba ponownie zwraca uwagę, że składając ofertę wraz z wymaganą próbką wykonawca zaakceptował sposób oceny próbki, a z wyniku oceny jego próbki nie może wywodzić wady powodującej niemożność zawarcia umowy skutkującej koniecznością unieważnienia postępowania o udzielenie zamówienia publicznego. Warto też zauważyć – na które to okoliczności zwracał uwagę Zamawiający i Uczestnik - zasady dostarczenia próbki zostały precyzyjnie określone w załączniku nr 8 do SWZ – OPZ. W punkcie bowiem 144 wskazano, że taka próbka ma być dostarczona wraz z ofertą i odpowiednią dokumentacją. Wskazano także na sposób oceny podając, że weryfikacja zgodności oferowanego sytemu nastąpi poprzez porównanie ze wszystkim wymaganiami. Wynik tej weryfikacji nie był arbitralny, albowiem wykonawca był uprawniony po otrzymaniu wyników oceny na zdalnym spotkaniu odnieść się do wyników oceny zgodności i intuicyjności systemu z uwagi na wskazane w punkcie 145 kryterium. Tym samym to kryterium, wobec którego na tym etapie postępowania jest podnoszony zarzut, nie prowadziło do subiektywnego – arbitralnego - eliminowania przez Zamawiającego ofert wykonawców. Wykonawcy mieli bowiem prawo po przeprowadzeniu oceny oferowanych systemów informatycznych odnieść się do wyników tej oceny. Tym samym nie można zgodzić się z twierdzeniami Odwołującego w świetle argumentacji odwołania i okoliczności wskazanych, że opis przedmiotu jest wewnętrznie sprzeczny i niejednoznaczny, co nie pozwalało na prawidłową ocenę ofert, oraz dawało Zamawiającemu prawo subiektywnej (czytaj: arbitralnej) oceny niezgodności systemu z jego oczekiwaniami.

Wobec powyższego także ten zarzut Izba uznała za niezasadny.

W konkluzji Izba stwierdza, że w przypadku oferty Odwołującego nie potwierdziły się zarzuty naruszenia art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) - 3) ustawy Pzp, oraz (2) art. 226 ust. 1 pkt 8) w zw. z art. 224 ust. 6 ustawy Pzp, a także zarzut w odniesieniu do oferty wykonawcy TK-MED – naruszenia art. 226 ust. 1 pkt 5) w zw. z art. 16 pkt 1) - 3) ustawy Pzp. Także za podlegający oddaleniu Izba uznała zarzut ewentualny zaniechania unieważnienia przedmiotowego postępowania z naruszeniem art. 255 pkt 6) w zw. z art. 457 ust. 1 pkt 1) w zw. z art. 99 ust. 1 i 4 i w zw. z art. 16 pkt 1) i 2) ustawy Pzp. Tym samym także zarzut naruszenia art. 239 ust. 1 i 2 ustawy Pzp w związku z wyborem oferty TK-MED jako najkorzystniejszej nie podlega uwzględnieniu.

O kosztach postępowania orzeczono stosownie do wyniku na podstawie art. 575 ustawy - Prawo zamówień publicznych oraz w oparciu o przepisy poz. 2437).

Mając powyższe na uwadze, Krajowa Izba Odwoławcza orzekła jak w sentencji wyroku.

……