**Sygn. akt:KIO 3399/23**

**KIO 3427/23**

**WYROK**
**z dnia 1 grudnia 2023 r.**

**Krajowa Izba Odwoławcza** – w składzie:

Przewodniczący: Krzysztof Sroczyński
Maria Kacprzyk
Maksym Smorczewski
Protokolant: Klaudia Kwadrans

po rozpoznaniu na rozprawie w dniu 29 listopada 2023 r. w Warszawie odwołań wniesionych do Prezesa Krajowej Izby Odwoławczej w dniu 13 listopada 2023 r. przez:
A)wykonawcę FINTECH spółkę akcyjną z siedzibą w Warszawie przy ul. Kaszmirowej 1/2 (03-991 Warszawa) – sprawa o sygn. akt KIO 3399/23;
B) wykonawcę Integrated Solutionsspółkę z ograniczoną odpowiedzialnością z siedzibą w Warszawie przy ul. Karolkowej 30 (01-207 Warszawa) – sprawa o sygn. akt: KIO 3427/23;

w postępowaniu, w którym zamawiającym jest Sąd Apelacyjny w Krakowie przy ul. Przy Rondzie 3 (31-547 Kraków) , a prowadzącym postępowanie Centrum Zakupów dla Sądownictwa Instytucja Gospodarki Budżetowej z siedzibą w Krakowie przy ul. Wadowickiej 6 (30-415 Kraków)

przy udziale:
- wykonawcy PASSUS spółka akcyjna z siedzibą w Warszawie ul. Goraszewska 19, (02-910 Warszawa), zgłaszającego przystąpienia do postępowania odwoławczego w sprawach o sygn. akt KIO 3399/23 i KIO 3427/23 po stronie zamawiającego;
- wykonawcy FINTECH spółka akcyjna z siedzibą w Warszawie przy ul. Kaszmirowej 1/2 (03-991 Warszawa), zgłaszającego przystąpienie do postępowania odwoławczego w sprawie o sygn. akt KIO 3427/23 po stronie odwołującego

**orzeka:**

umarza postępowanie odwoławcze o sygn. KIO 3399/23 w zakresie w jakim zarzut dotyczył postanowień pkt 1 ppkt 5, ppkt 6 i ppkt 16, pkt 2 ppkt 19, pkt 6 ppkt 22 oraz pkt 8 ppkt 1 i 6 Szczegółowego Opisu Przedmiotu Zamówienia stanowiącego załącznik nr 2 Specyfikacji Warunków Zamówienia

oddala odwołanie w postępowaniu odwoławczym sygn. akt KIO 3399/23 w pozostałym zakresie;

uwzględnia odwołanie w postępowaniu odwoławczym sygn. akt KIO 3427/23 w części, uznając za uzasadniony zarzut naruszenia art. 99 ust. 4 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych w zakresie dotyczącym postanowienia pkt 1 ppkt 1 Szczegółowego Opisu Przedmiotu Zamówienia, stanowiącego załącznik nr 2 Specyfikacji Warunków Zamówienia (zarzut 3a odwołania) i nakazuje zamawiającemu usunięcie tego postanowienia;

oddala odwołanie w postępowaniu odwoławczym sygn. akt KIO 3427/23 w pozostałym zakresie;

kosztami postępowania odwoławczego o sygn. akt KIO 3399/23 obciąża odwołującego– FINTECH spółkę akcyjną z siedzibą w Warszawie, i:

5.1zalicza w poczet kosztów postępowania kwotę 15 000 zł (słownie: piętnastu tysięcy złotych) uiszczoną przez odwołującego - FINTECH spółkę akcyjną z siedzibą w Warszawie tytułem wpisu od odwołania,

5.2zasądza od odwołującego – FINTECH spółki akcyjnej z siedzibą w Warszawie na rzecz zamawiającego – Sądu Apelacyjnego w Krakowie kwotę 3 600 zł (słownie: trzy tysiące sześćset złotych) stanowiącą uzasadnione koszty zamawiającego poniesione tytułem kosztów wynagrodzenia pełnomocnika.

osztami postępowania odwoławczego sygn. akt KIO 3427/23 obciąża odwołującego - Integrated Solutions spółkę z ograniczoną odpowiedzialnością z siedzibą w Warszawie w 3/4 części oraz zamawiającego Sąd Apelacyjny w Krakowie w 1/4 części i:

6.1. zalicza na poczet kosztów postępowania odwoławczego kwotę 15 000 zł (słownie: piętnaście tysięcy złotych) uiszczoną przez odwołującego - Integrated Solutions spółkę z ograniczoną odpowiedzialnością z siedzibą w Warszawie tytułem wpisu od odwołania;

6.2. zasądza od zamawiającego - Sądu Apelacyjnego w Krakowie na rzecz odwołującego - Integrated Solutions spółki z ograniczoną odpowiedzialnością z siedzibą w Warszawie kwotę w wysokości 1 050 zł (słownie: jeden tysiąc pięćdziesiąt złotych) stanowiącą różnicę pomiędzy kosztami postępowania odwoławczego, a kosztami postępowania za jakie odpowiadał Odwołujący w świetle jego wyniku.

Stosownie do art. 579 ust. 1 i 580 ust. 1 i 2 ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2023 r., poz. 1605 ze zm.) na niniejszy wyrok – w terminie 14 dni od dnia jego doręczenia – przysługuje skarga za pośrednictwem Prezesa Krajowej Izby Odwoławczej do Sądu Okręgowego w Warszawie.

Przewodniczący:…….
…….
…….

**Sygn. akt:KIO 3399/23**

**KIO 3427/23**

**U z a s a d n i e n i e**

Centrum Zakupów dla Sądownictwa Instytucja Gospodarki Budżetowej z siedzibą w Krakowie, działając na rzecz Sądu Apelacyjnego w Krakowie, zwanego dalej „zamawiającym”, na podstawie art. 311 ust. 1 pkt 1) ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t. j. Dz. U. z 2023 r., poz. 1605 ze zm.), zwanej dalej: „Pzp”, prowadzi postępowanie o udzielenie zamówienia publicznego w celu zawarcia umowy ramowej z odpowiednim stosowaniem przepisów dotyczących trybu przetargu nieograniczonego pn.: *Umowa ramowa na dostawę*

*rozwiązania informatycznego obejmującego funkcjonalność zarządzania informacją i zdarzeniami bezpieczeństwa SIEM/SOAR oraz świadczenie innych usług towarzyszących")"* o numerze: WZP-421-16/2023, zwane dalej: „postępowaniem".

Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej w dniu 2 listopada 2023 r. pod numerem 2023/S 211- 00666319.

Szacunkowa wartość zamówienia, jest wyższa od kwot wskazanych w przepisach wykonawczych wydanych na podstawie art. 3 ust. 2 Pzp.

**Sygn. akt KIO 3399/23**

W dniu 13 listopada 2023 r. wykonawca FINTECH S.A. z siedzibą w Warszawie(zwany dalej: „Odwołującym1" lub „Odwołującym FINTECH")wniósł odwołanie wobec treści dokumentów zamówienia, to jest Szczegółowego Opisu Przedmiotu Zamówienia (dalej: SOPZ) stanowiącego Załącznik nr 2 do Specyfikacji Warunków Zamówienia, których treść ukształtowała aktualny opis przedmiotu i warunków zamówienia w sposób niezgodny z ustawą PZP w zakresie:

I. Pkt. 1 ppkt. 5 SOPZ o treści: „System SIEM musi umożliwiać wykorzystanie w innych obszarach niż zarządzanie informacją bezpieczeństwa w oparciu o wspólne dane w szczególności w zakresie: 5.1monitorowania infrastruktury 5.2 monitorowania dostępności usług 5.3 wydajności aplikacji.5.4 Monitorowanie procesów biznesowych";

II. Pkt. 1 ppkt. 6 SOPZ o treści: „System SIEM musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych obejmujących: 6.1 mechanizmy pobierania danych, 6.2.raporty, dashboardy i formularze, 6.3 nowe funkcje analityczne, 6.4 nowe sposoby wizualizacji, 6.5 mechanizmy powiadamiania" powielony i rozszerzony w pkt. 6 ppkt. 23 SOPZ o treści: „System SIEM musi umożliwiać tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych obejmujących: 23.1mechanizmy pobierania danych, 23.2 raporty, dashboardy i formularze, 23.3 nowe funkcje analityczne, 23.4 nowe sposoby wizualizacji, 23.5 mechanizmy powiadamiania, w tym dwukierunkowe – inne niż przewidział producent. Realizacja tych funkcjonalności nie może wymagać konieczności angażowania Producenta i nie może naruszać praw autorskich. Komponenty oferowanego rozwiązania w obszarze analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych nie muszą pochodzić od jednego Producenta, jednak nie mogą być to rozwiązania open source.";

III. Pkt. 1 ppkt. 16 SOPZ o treści: „System SIEM musi posiadać wbudowane mechanizmy kompresji danych przetwarzanych online na zasobach dyskowych na poziomie minimum 30% w stosunku do wielkości otrzymywanych danych."

IV. Pkt. 2 ppkt. 13 SOPZ o treści: „Agent musi mieć możliwość równoważenia obciążenia(wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie"

V. Pkt. 2 ppkt 16 SOPZ o treści: „Rozwiązanie powinno zapewniać dostępność agentów, udostępnionych przez Producenta rozwiązania, do zbierania zdarzeń z serwerów z systemami operacyjnymi Microsoft Windows, Unix/Linux, lub innych serwerów aplikacyjnych, bez konieczności wnoszenia dodatkowych opłat lub zawierać odpowiedni pakiet licencji, gwarantujący możliwość zainstalowania stosownego agenta na każdym z potencjalnych źródeł, które Jednostki będą chciały podłączyć do Systemu SIEM."

VI. Pkt. 2 ppkt. 18 SOPZ o treści: „Oprócz źródeł wymienionych wyżej System SIEM musi umożliwiać pobieranie informacji z wykorzystaniem poniższych mechanizmów: 18.1 dane wydajnościowe Windows Performance Monitor, 18.2 dowolne dane WMI, 18.3 wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym, 18.4 Zmiany w zawartości plików i kluczy rejestrów. 18.5 Pliki tekstowe na zdalnych serwerach poprzez SSH, CIFS i NFS."

VII. Pkt. 2 ppkt. 19 SOPZ o treści: „System SIEM musi umożliwiać parsowanie logów o długości co najmniej 10 000znaków oraz zawierających więcej niż jedną linię."

VIII. Pkt. 3 ppkt. 3 SOPZ o treści: „Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach: a) Katalogi LDAP, b) Bazy danych, c) Bazy no SQL d) Hadoope) Dane geolokalizacyjne."

IX. Pkt. 4 ppkt. 4 SOPZ o treści: „Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych. Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem."

X. Pkt. 5 ppkt. 12 SOPZ o treści: „System SIEM musi umożliwiać konfigurację klastrów wysokiej dostępności z równoważeniem obciążenia(klastry Active/Active). Musi istnieć możliwość konfiguracji dowolnej liczby węzłów klastra. Równoważenie obciążenia pomiędzy komponentami systemu SIEM nie może wymagać stosowania zewnętrznego rozwiązania je rozkładającego (tzw. Loadbalancer) oraz nie może wymagać zakupu żadnej dodatkowej licencji."

XI. Pkt. 6 ppkt. 6 SOPZ o treści: „System SIEM musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej: 6.1 Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych, 6.2 Możliwość przypisania incydentu do osoby, 6.3 Możliwość zmiany statusu i priorytetu incydentu, 6.4 Możliwość tworzenia komentarzy, 6.5 Możliwość automatycznego i ręcznego modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy. 6.6Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki. 6.7 Możliwość raportowania wydajności obsługi incydentów."

XII. Pkt. 6ppkt. 22 SOPZ o treści: „System SIEM powinien cechować się uniwersalnością, tzn. oprócz funkcjonalności dedykowanych bezpieczeństwu, powinien zapewniać możliwość wykorzystania wybranego rozwiązania do analityki biznesowej, raportowania, monitoringu infrastruktury teleinformatycznej oraz zarządzania i monitoringu logów systemowych i aplikacyjnych."

XIII. Pkt. 8 ppkt. 1 SOPZ o treści: „System SOAR musi zapewniać możliwości orkiestracji i automatyzacji bezpieczeństwa oraz odpowiedzi na incydent , które natywnie (tj. poprzez wbudowaną funkcjonalność i możliwości) w pełni integrują się z większością technologii bezpieczeństwa na rynku."

XIV. Pkt. 8 ppkt. 6 SOPZ o treści: „System SOAR musi zapewniać kontrolę wersji dostępnych scenariuszy (playbooks)."

Zaskarżonym czynnościom zamawiającego, Odwołujący1 zarzucił naruszenie art. 99 ust. 1, 2 i 4 PZP w zw. z art. 16 PZP przez dokonanie opisu przedmiotu zamówienia zawartego w SOPZ przez odniesienie się do cech dostaw w sposób nieproporcjonalny do celu zamówienia oraz w sposób utrudniający uczciwą konkurencję, przez dobór parametrów technicznych i preferencje określonych rozwiązań technicznych, które charakteryzują produkty dostarczane przez jednego wykonawcę, doprowadzając przy tym do wyeliminowania producentów oprogramowania innego niż Splunk i wykonawców oferujących inne rozwiązania.

Wobec powyższego, Odwołujący1 wniósł o rozpatrzenie i uwzględnienie odwołania oraz nakazanie

zamawiającemu zmiany treści SOPZ oraz dokumentów zamówienia, w sposób zgodny z przepisami PZP, w szczególności z wskazanymi wyżej przepisami art. 16 i 99 PZP w następujący sposób:
Ad. I – wykreślenie w całości wymagania opisanego w pkt. 1 ppkt. 5 SOPZ
Ad. II – wykreślenie w całości wymagania opisanego pkt. 1 ppkt. 6 SOPZ oraz zmianę pkt. 6 ppkt. 23 SOPZ w następujący sposób: „*System SIEM musi umożliwiać, pod warunkiem braku ingerencji w kod źródłowy systemu SIEM i nienaruszania praw autorskich i patentowych, tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych z wykorzystaniem zewnętrznych komponentów komercyjnych obejmujących: 23.1mechanizmy pobierania danych, 23.2 raporty, dashboardy i formularze, 23.3 nowe funkcje analityczne, 23.4 nowe sposoby wizualizacji, 23.5 mechanizmy powiadamiania, w tym dwukierunkowe - inne niż przewidział producent. Realizacja tych funkcjonalności przez Jednostki będzie wymagać konieczności angażowania Producenta i nie może naruszać jego praw autorskich*."
Ad. III – zmianę pkt. 1 ppkt. 16 SOPZ w następujący sposób:„*System SIEM musi posiadać wbudowane mechanizmy kompresji danych przetwarzanych online na zasobach dyskowych na poziomie minimum 30% w stosunku do wielkości otrzymywanych danych lub ograniczania ilości danych przetwarzanych online przed rozpoczęciem ich przetwarzania za pomocą filtracji lub selekcji danych na urządzeniach kolekcjonujących zdarzenia*."
Ad. IV – wykreślenie w całości wymagania opisanego w pkt. 2 ppkt. 13 SOPZ
Ad. V – zmianę pkt. 2 ppkt 16 SOPZ w następujący sposób: „*Rozwiązanie powinno zapewniać dostępność agentów, udostępnionych przez Producenta rozwiązania, do zbierania zdarzeń z serwerów z systemami operacyjnymi Microsoft Windows, Unix/Linux, lub innych serwerów aplikacyjnych, bez konieczności wnoszenia dodatkowych opłat lub zawierać odpowiedni pakiet licencji, gwarantujący możliwość zainstalowania stosownego agenta na każdym z możliwych do podłączenia źródeł, które Jednostki będą chciały podłączyć do Systemu SIEM*."
Ad. VI – zmianę pkt. 2 ppkt. 18 SOPZ w następujący sposób: „*Oprócz źródeł wymienionych wyżej System SIEM musi umożliwiać pobieranie informacji z wykorzystaniem poniższych mechanizmów: 18.1 dane wydajnościowe Windows Performance Monitor, 18.2 dowolne dane WMI, 18.3 wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie źródłowym, 18.4 Zmiany w zawartości plików i kluczy rejestrów. 18.5 Pliki tekstowe na zdalnych serwerach poprzez CIFS i NFS*."
Ad. VII – zmianę pkt. 2 ppkt. 19 SOPZ w następujący sposób: „*System SIEM musi umożliwiać parsowanie logów o długości do 10 000 znaków oraz zawierających więcej niż jedną linię*."
Ad. VIII – zmianę pkt. 3 ppkt. 3 SOPZ w następujący sposób:„*Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach: a) Katalogi LDAP, b) Bazy danych, c) Bazy no SQL np. za pośrednictwem plików płaskich CSV d) Hadoop np. za pośrednictwem plików płaskich CSV e) Dane geolokalizacyjne*."
Ad. IX – wykreślenie w całości wymagania opisanego w pkt. 4 ppkt. 4 SOPZ
Ad. X – zmianę pkt. 5 ppkt. 12 SOPZ w następujący sposób: „*System SIEM musi umożliwiać konfigurację klastrów wysokiej dostępności zrównoważeniem obciążenia. Równoważenie obciążenia pomiędzy komponentami systemu SIEM może zostać zrealizowane z wykorzystaniem zewnętrznego rozwiązania je rozkładającego (tzw. loadbalancer)*."
Ad. XI – zmianę pkt. 6 ppkt. 6 SOPZ w następujący sposób: „*System SIEM oraz System SOAR muszą zapewniać (razem lub osobno) mechanizmy zarządzania incydentami obejmujące co najmniej: 6.1 Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych, 6.2 Możliwość przypisania incydentu do osoby, 6.3 Możliwość zmiany statusu i priorytetu incydentu, 6.4Możliwość tworzenia komentarzy, 6.5 Możliwość modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy. 6.6 Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki. 6.7 Możliwość raportowania wydajności obsługi incydentów*."
Ad. XII – wykreślenie w całości wymagania opisanego w pkt. 6 ppkt. 22 SOPZ
Ad. XIII – wykreślenie w całości wymagania opisanego w pkt. 8 ppkt.1 SOPZ
Ad. XIV – zmianę Pkt. 8 ppkt. 6 SOPZ w następujący sposób:„*System SOAR musi zapewniać możliwość kontroli wersji dostępnych scenariuszy (playbooks) w postaci automatycznego lub ręcznego wersjonowania*."
Ponadto Odwołujący1 wniósł o:
- nakazanie zamawiającemu niezwłocznego przekazania wszystkim wykonawcom zmiany dokumentacji postępowania za pośrednictwem strony internetowej postępowania, na której jest udostępniana,
- nakazanie zamawiającemu przesunięcia terminu składania ofert, stosownie do treści art. 137 ust. 6 PZP, o czas niezbędny na zapoznanie się ze zmianą SWZ i przygotowanie oferty oraz
- orzeczenie na rzecz Odwołującego1 zwrotu uzasadnionych kosztów postępowania odwoławczego, w tym wynagrodzenia pełnomocnika oraz kosztów dojazdu na rozprawę, określonych na podstawie rachunków, który zostaną przedłożone do akt sprawy.

Odwołujący1 wyjaśnił, że ma interes w uzyskaniu zamówienia będącego przedmiotem postępowania, gdyż prowadzi działalność gospodarczą sklasyfikowaną w PKD jako 62.01.Z - działalność związana z oprogramowaniem, 62.02.Z – działalność związana z doradztwem w zakresie informatyki oraz 62.09 - pozostała działalność usługowa w zakresie technologii informatycznych i komputerowych. Ponadto odwołujący planuje wziąć udział w postępowaniu, w przedmiocie którego składa odwołanie. Należy zwrócić uwagę, że zgodnie z doktryną i orzecznictwem KIO biorąc pod uwagę brzmienie art. 505 ust. 1 PZP, chodzi tu o posiadanie jakiegokolwiek interesu, w tym istnienie uzasadnienia dla prowadzenia postępowania odwoławczego wynikającego z dążenia do uzyskania korzystniejszych warunków zawarcia umowy, ale również interesu nakierowanego na uzyskanie zamówienia, którego wykonawca nie uzyskałby, gdyby zaniechał wniesienia środka ochrony prawnej (tak wyrok KIO z dnia 26 stycznia 2011 r., KIO 93/11, www.uzp.gov.pl) (A. Bazan, Prawo Zamówień Publicznych. Komentarz, wyd. II, Komentarze LEX 2015). Przesłanką legitymacji do wniesienia odwołania jest również możliwość poniesienia szkody w wyniku naruszenia przez zamawiającego przepisów PZP. Istotnym jest, że odwołujący, składając ofertę w przedmiotowym postępowaniu musi ponieść określony wysiłek, angażując przy tym czas pracy i umiejętności swoich pracowników odpowiedzialnych za przygotowanie jej w sposób umożliwiający uznanie jej przez zamawiającego za ofertę najkorzystniejszą, narażając się przy tym na możliwość poniesienia szkody wynikającej z niemożności składania ofert w- innych postępowaniach tudzież podejmowania zleceń od podmiotów prywatnych. Jednocześnie w wyniku naruszenia przez zamawiającego przepisów ustawy szkoda po stronie Odwołującego1 może polegać na uniemożliwieniu złożenia oferty zgodnej ze wszystkimi postanowieniami SWZ. W rezultacie Odwołujący1 nie będzie mógł uzyskać przedmiotowego zamówienia i osiągnąć zysku.

W uzasadnieniu zarzutów, Odwołujący1 w pierwszej kolejności podkreślił, że w przypadku podniesienia zarzutów naruszenia przez Zamawiającego art. 99 ust. 4 oraz art. 16 pkt 1 PZP, od wykonawcy składającego odwołanie wymagane jest jedynie uprawdopodobnienie, że Zamawiający sporządził SWZ niezgodnie z zasadami określonymi w tych przepisach, a nie udowodnienie tej okoliczności. Ciężar dowodu w zakresie braku istnienia ograniczenia konkurencji w Postępowaniu spoczywa na Zamawiającym. To Zamawiający powinien przedstawić dowód przeciwny podniesionym przez Odwołującego twierdzeniom. Zamawiający powinien wskazać, że zaskarżone przez Odwołującego wymaganie nie narusza zasady uczciwej konkurencji, równego traktowania wykonawców oraz proporcjonalności. Potwierdzeniem w tym

zakresie jest orzecznictwo Krajowej Izby Odwoławczej. Przykładowo, w wyroku z dnia 20 sierpnia 2018 r. (sygn. akt KIO 1518/18) Izba wskazała, że „(…) fakt naruszenia przez zamawiającego przepisów art. 7ust. 1 oraz art. 29 ust. 2 ustawy PZP [aktualnie art. 99 ust. 4 PZP] wymaga jedynie uprawdopodobnienia (….) w konsekwencji ciężar dowodu w zakresie braku zaistnienia ograniczenia konkurencji w postępowaniu spoczywa na zamawiającym. Dowód taki jest skutecznie przeprowadzony jeżeli zamawiający wykaże, że odwołujący spełnia ustalone wymagania lub, że mimo braku spełnienia tych wymagań opis przedmiotu zamówienia uzasadniony jest szczególnymi potrzebami zamawiającego. (…) wykazanie wymagać musi odbyć w sposób wiarygodny, logiczny i spójny, przez wyspecyfikowanie co było podstawą takich a nie innych wymagań. Naturalnie nie może stanowić takiego uzasadnienia jak miało to miejsce w tym przypadku jedynie gołosłowne oświadczenie zamawiającego". Analogicznie, w wyroku z dnia 2 grudnia 2010 r. (sygn. akt KIO 2528/10) Izba orzekła, że „zgodnie z utrwalonym w orzecznictwie stanowiskiem dla uznania zasadności zarzutu naruszenia tych przepisów wystarczające jest uprawdopodobnienie przez wykonawcę możliwości ograniczenia konkurencji przez dokonany przez zamawiającego opis przedmiotu zamówienia. (…) Jednocześnie Izba podziela wyrażony również w orzecznictwie pogląd, iż w razie postawienia zamawiającemu zarzutu naruszenia przepisu art. 29 ust. 2 to na nim spoczywa ciężar udowodnieni, iż zawarty w s.i.w.z. opis przedmiotu zamówienia nie został sformułowany w sposób, który mógłby utrudniać uczciwą konkurencję". Zamawiający może skutecznie zakwestionować zarzut naruszenia art. 99 ust. 4 PZP jeśli wykaże, że opis przedmiotu zamówienia ma źródło w jego uzasadnionych potrzebach. Biorąc pod uwagę zapis art. 99 ust. 4 ustawy PZP, zgodnie z którym przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, wystarczy do stwierdzenia faktu nieprawidłowości w opisie przedmiotu zamówienia, a tym samym sprzeczności z prawem, jedynie zaistnienie możliwości utrudniania uczciwej konkurencji poprzez zastosowanie określonych zapisów w specyfikacji (zob. Wyrok SO w Bydgoszczy z dnia 25 stycznia 2006 r., II Ca 693/5).

Szczegółowa analiza wymagań SOPZ wskazuje na istotne ograniczenie grupy producentów systemów SIEM i SOAR, którzy mogą wziąć udział w postępowaniu. Wymaganie pisane w pkt. 1 ppkt. 1 SOPZ o treści: „System SIEM musi być dojrzałym, uznanym na rynku produktem – jako potwierdzenie spełnienia wymagania uznane będzie: (...) zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert) lub (...) oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert)." ogranicza grupę potencjalnych oferentów do firm: Splunk, Microsoft, Elastic, IBM, Securonix, Exabeam. Odwołujący1 przedstawił zestawienie wyników najnowszych dostępnych raportów firm badawczych Gartner oraz Forrester Research: https://www.splunk.com/en_us/form/gartner-siem-magic-quadrant.htmlhttps://logrhythm.com/gartner-magic-quadrant-siem-report-2022/https://www.microsoft.com/en-us/security/blog/2022/10/13/microsoft-named-a-leader-in-the-2022-gartner-magic-quadrant-for-security-information-and-event-management/https://www.splunk.com/en_us/form/forrester-wave-security-analytics-platforms.htmlhttps://www.microsoft.com/en-us/security/blog/2022/12/19/forrester-names-microsoft-a-leader-in-q4-2022-security-analytics-platforms-wave-report/https://www.elastic.co/explore/security-without-limits/forrester-analyst-security-analytics-wave-report

Wymaganie opisane w pkt. 1 ppkt. 2 SOPZ o treści: „Nie dopuszcza się rozwiązań open source." wyklucza z wyżej wymienionej grupy producentów rozwiązanie firmy Elastic. Wymaganie opisane w pkt. 1 ppkt. 4 SOPZ o treści: „System SIEM musi spełniać wymogi bezpieczeństwa Common Criteria for IT Security Evaluation potwierdzone certyfikatem wydanym nie wcześniej niż w 2020 roku przez akredytowane laboratorium Common Criteria." jest spełnione jedynie przez dwóch producentów z wyżej wymienionej listy, tj. przez Splunk (numer raportu certyfikacyjnego CCEVS-VR-VID11330-2023, 23 marca 2023) i IBM (numer raportu certyfikacyjnego CCEVS-VR-VID11376-2023, 5 lipca 2023). Pełen wykaz producentów i ich rozwiązań certyfikowanych przez Common Criteria można znaleźć w https://www.commoncriteriaportal.org/products/index.cfm. Analiza kolejnych wymagań SOPZ względem rozwiązań producentów Splunk i IBM wskazuje, że jedynym producentem mogącym wziąć udział w postępowaniu pozostaje Splunk: 1.wymaganie w pkt. 5 ppkt. 12 2. wymaganie w pkt. 6 ppkt. 22. Należy przy tym podkreślić, że w opinii niezależnych ekspertów ds. bezpieczeństwa rozwiązanie Splunk jest zasadniczo zaawansowanym narzędziem wyszukiwania przeznaczonym dla działów IT, nie jest typowym systemem SIEM, a jedynie oferuje takie rozszerzenie funkcjonalności. Opinia ta znajduje również odzwierciedlenie w certyfikacji Common Criteria dla tego rozwiązania, które sklasyfikowane jest w kategorii „Inne urządzenia i systemy" (ang. „Other devices and systems"). W opinii Odwołującego1 rozwiązanie Splunk ogranicza automatyczną korelację zdarzeń, przez co zespoły ds. bezpieczeństwa są zmuszone do ręcznej korelacji, co jest skomplikowane, czasochłonne i może prowadzić do wydłużenia czasu analizy. Rozwiązanie nie zapewnia korelacji zdarzeń w czasie rzeczywistym. Budowa reguł korelacyjnych w Splunk to w rzeczywistości budowa zapytań bazodanowych uruchamianych dopiero po tym, jak dane trafią do bazy (istnieje zatem ryzyko opóźnień w analizie, co może w konsekwencji mieć skutek w opóźnionej reakcji na incydent). W dodatku Splunk umożliwia jedynie manualne „sekwencjonowanie zdarzeń" dla jedynie określonych reguł, co dodatkowo komplikuje analizę złożonych incydentów. Dalej, Splunk nie zapewnia również wystarczającej widoczność aktywności sieciowych. Zaawansowani napastnicy często wyłączają logowanie zdarzeń, dzięki czemu mogą pozostać w ukryciu. „Strumienie" Splunk do pozyskiwania przepływów sieciowych (flows) są ograniczone i nie obejmują poziomu analizy kryminalistycznej sieci QNI, który jest wymagany do wykrywania zaawansowanych ataków. Ponadto zbudowany dla DevOps system Splunk w zakresie specjalistycznej wiedzy w dziedzinie cyberbezpieczeństwa opiera się na możliwościach firm trzecich. W odróżnieniu do innych producentów Splunk nie dysponuje dedykowaną specjalistyczną jednostką cyberthreat intelligence, która stale monitoruje zagrożenia w cyberprzestrzeni i dostarcza automatycznie do systemu SIEM wiedzy o aktualnych zagrożeniach (tzw. threat intelligence). W przypadku kradzieży poświadczeń użytkownika zaatakowane systemy często komunikują się z niezaufanymi hostami zewnętrznymi. Wykrywając te połączenia i zwiększając współczynnik ryzyka użytkownika, zaatakowanych użytkowników można wykryć znacznie szybciej. Bez tej wbudowanej i skorelowanej analizy zagrożeń napastnicy mogą pozostać w ukryciu dłużej, co zwiększa prawdopodobieństwo skutecznej eksfiltracji danych. Splunk również w tym zakresie całkowicie polega na informacjach o zagrożeniach pochodzących od firm trzecich.

Ponadto odnosząc się do zarzutów wymienionych w odwołaniu, Odwołujący1 wskazał, co następuje: Ad. I – Systemy SIEM zgodnie z powszechnie obowiązującą definicją oraz scenariuszami zastosowania nie służą wymienionym w wymaganiu działaniom. Producenci systemów SIEM mogą rozszerzać funkcjonalność poprzez dołączanie dodatkowych komponentów, które takie działania będą realizować, jednak nie jest to powszechna praktyka ze względu na fakt, iż istnieją na rynku specjalistyczne narzędzia do realizacji takich działań, np. Zabbix (monitorowanie infrastruktury, monitorowanie dostępności usług), Cisco AppDynamics (wydajność aplikacji, monitorowanie procesów biznesowych). Producenci SIEM zazwyczaj umożliwiają integrację z takimi rozwiązaniami.

Ad. II – Producenci komercyjnych systemów SIEM udostępniają integracje z zewnętrznymi narzędziami, które mogą rozszerzać funkcjonalność poprzez dołączanie dodatkowych komponentów, jednocześnie udzielane licencje oprogramowanie nie dopuszczają do samodzielnego tworzenia nowych funkcjonalności w ramach ich systemów ze

względu na naruszenie praw autorskich i patentowych. Stawianie takiego wymagania istotnie ogranicza grupę producentów SIEM (lub wręcz wyklucza wszystkich producentów komercyjnych systemów SIEM), chcących wziąć udział w postępowaniu.
Ad. III –Kompresja danych przetwarzanych on-line nie jest rekomendowana ze względu ryzyko ograniczenia wydajności systemu SIEM oraz w konsekwencji wydłużenia czasu reakcji na incydent. Ograniczanie ilości danych on-line można zrealizować metodami filtracji lub selekcji na urządzeniach kolekcjonujących zdarzenia przed procesem ich przetwarzania.
Ad. IV – Wymaganie dot. równoważenia obciążenia według najlepszych praktyk jest realizowane na urządzeniach kolekcjonujących dane (centralnych), a nie na agentach zainstalowanych na urządzeniach dostarczających dane. Funkcjonalność równoważenia obciążenia jest zazwyczaj realizowana za pośrednictwem tzw. load-balancer'ów, umieszczanych w architekturze przed urządzeniami kolekcjonującymi dane. Wymaganie realizacji takiej funkcjonalności na agentach istotnie ogranicza grupę producentów SIEM mogących wziąć udział w postępowaniu, a dodatkowo obciąża systemy źródłowe, w tym systemy infrastruktury krytycznej.
Ad. V – SOPZ nie specyfikuje źródeł, które Jednostki mogą potencjalnie chcieć podłączyć do Systemu SIEM. Producenci systemów SIEM umożliwiają podłączanie całej gamy źródeł, zapewniając w ten sposób szerokie możliwości analityczne, niemniej nie jest możliwe, aby w tym zakresie pozostawała nieograniczona dowolność. Możliwość podłączenia niestandardowego źródła danych jest z reguły dostępna, jednak musi ona być zweryfikowana na etapie analizy przedwdrożeniowej systemu.
Ad. VI – Logowanie po SSH nie jest rekomendowane przez ekspertów ds. bezpieczeństwa, nie jest to dobra praktyka ze względu na ryzyko wycieku poświadczeń.
Ad. VII – Wymaganie tej treści istotnie ogranicza grupę producentów systemów SIEM, chcących wziąć udział w postępowaniu. Większość producentów SIEM umożliwia parsowanie logów o długości co najwyżej 10000 znaków. W praktyce nie spotyka się systemów źródłowych, które generują logi o większej liczbie znaków.
Ad. VIII – Ze względu na charakterystykę niestrukturyzowanych lub nierelacyjnych baz danych noSQL i Hadoop wymaganie wymaga doprecyzowania. Producenci SIEM stosują metody integracji ze tego typu źródłami, najczęściej poprzez normalizację danych do plików płaskich CSV. Istnieje jedynie wąska grupa producentów SIEM, którzy wykorzystują integrację natywną.
Ad. IX – Zamawiający w pkt. 1 ppkt. 4 stawia wymaganie zgodności z wymogami bezpieczeństwa Common Criteriafor IT Security Evaluation, potwierdzone certyfikatem wydanym nie wcześniej niż w 2020roku przez akredytowane laboratorium Common Criteria. W przypadku systemów SIEM, które posiadają certyfikację Common Criteria nie jest wymagane dodatkowe szyfrowanie danych. Aby uzyskać certyfikat zgodności z Common Critera systemy SIEM muszą być utwardzone według najlepszych obowiązujących praktyk (tzw. hardening) w celu eliminacji ryzyka ingerencji w poufność i integralność kodu źródłowego oraz przetwarzanych danych. Dodatkowe wymaganie na szyfrowanie danych wydaje się być nadmiarowe w świetle wymagania w pkt. 1 ppkt. 4 oraz może ograniczać grupę potencjalnych producentów systemów SIEM, chcących wziąć udział w postępowaniu.
Ad. X – Klastry active/active służą do zapewnienia wysokiej wydajności, a nie wysokiej dostępności. Producenci systemów SIEM zapewniają wysoką wydajność poprzez odpowiedni dobór i konfigurację zasobów. Równocześnie Zamawiający błędnie łączy wymaganie wysokiej dostępności zrównoważeniem obciążenia. Wymaganie funkcjonalności load balancing (równoważenie obciążenia), podobnie jak wymaganie klastra active/active oferuje bardzo ograniczona grupa producentów SIEM. Powszechną praktyką adresowania tego typu wymagania jest stosowanie zewnętrznego (sprzętowego lub wirtualnego) load balancer'a na poziomie sieci, który nie jest dopuszczony przez Zamawiającego.
Ad. XI – Wymaganie wymienia funkcjonalności, które są dostępne zarówno w systemach SIEM, jak i w systemach SOAR, w zależności od producenta. Systemy SIEM i SOAR z założenia są systemami komplementarnymi, współpracującymi ze sobą. Systemy SOAR najczęściej rozszerzają funkcjonalność systemu SIEM. SOPZ dotyczy postępowania zarówno na jeden jak i na drugi system. Ograniczenie tego wymagania jedynie do systemu SIEM istotnie ogranicza grupę producentów SIEM, którzy koncentrują się na funkcjonalnościach SIEM, ale zapewniają integrację z szeroką gamą producentów systemów SOAR.
Ad. XII – Systemy SIEM zgodnie z powszechnie obowiązującą definicją oraz scenariuszami zastosowania nie służą wymienionym w wymaganiu działaniom. Producenci systemów SIEM mogą rozszerzać funkcjonalność poprzez dołączanie dodatkowych komponentów, które takie działania będą realizować, jednak nie jest to powszechna praktyka ze względu na fakt, iż istnieją na rynku specjalistyczne narzędzia do realizacji takich działań. Stawianie wymagania „uniwersalności" systemu SIEM istotnie może ograniczać grupę oferentów, zwłaszcza że wymaganie to nie precyzuje, z jakimi „wybranym rozwiązaniem" system SIEM miałby współpracować.
Ad. XIII – Zamawiający w sformułowaniu „w pełni integrują się z większością technologii bezpieczeństwa na rynku" nie wskazuje precyzyjnie, o jakie technologie chodzi. Taka definicja wymagania stwarza szerokie pole do interpretacji i jednocześnie może wykluczać część producentów systemów SIEM.
Ad. XIV – Treść wymagania może zostać odczytana jako wymaganie Zamawiającego do zapewnienia funkcjonalności automatycznego wersjonowania scenariuszy. Taka funkcjonalność jest oferowana jedynie przez bardzo wąską grupę producentów SIEM. Większość systemów SIEM zapewnia manualne wersjonowanie scenariuszy poprzez funkcje powielania i nadawania unikalnej nazwy, która wskazuje na wersję scenariusza.

Przystąpienie do postępowania odwoławczego o sygn. akt 3399/23 po stronie zamawiającego zgłosił wykonawca PASSUS spółka akcyjna z siedzibą w Warszawie.

W dniu 28 listopada 2023 r. Zamawiający złożył do akt sprawy odpowiedź na odwołanie, w ramach której wnosił o oddalenie odwołania o sygn. akt KIO 3399/23 w całości i przywołał argumentację na poparcie swojego stanowiska, w tym w szczególności treść modyfikacji dokumentów zamówienia, której dokonano w dniu 27.11.2023 r.

**Sygn. akt KIO 3427/23**

W dniu 13 listopada 2023 r. wykonawca Integrated Solutions Sp. z o.o. z siedzibą w Warszawie(zwani dalej: „Odwołującym2" lub „Odwołującym IS") wniósł odwołanie na treść dokumentów zamówienia, podnosząc następujące zarzuty:

1. Opisanie przedmiotu zamówienia w sposób nieuwzględniający wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty z uwagi na zastrzeżenie wymagania, aby oferowany system SIEM spełniał wymogi bezpieczeństwa Common Criteria for IT Security Evaluation potwierdzone certyfikatem wydanym nie wcześniej niż w 2020 roku przez akredytowane laboratorium Common Criteria, co jest niemożliwe do zapewnienia dla aktualnych wersji produktów SIEM z uwagi na procedurę certyfikacji Common Criteria for IT Security Evaluation, co w połączeniu z wymogiem dostarczenia przez wykonawcę najnowszej wersji oprogramowania, prowadzi do tego, że wykonawca musi

zrealizować świadczenie niemożliwe, co stanowi naruszenie art. 99 ust. 1 Pzp;

2. Żądanie przedmiotowych środków dowodowych, które nie są proporcjonalne, ani związane z przedmiotem zamówienia, z uwagi na konieczność złożenia certyfikatu Common Criteria dla aktualnej wersji systemu SIEM, co z uwagi na sposób certyfikacji Common Criteria nie jest możliwe i który to przedmiotowy środek dowodowy nie jest adekwatny do potwierdzenia spełniania przez oferowane dostawy wymagań Zamawiającego, gdyż obejmuje jedynie starsze wersje oprogramowania, co stanowi naruszenie art. 106 ust. 2 Pzp;

3. Opisanie przedmiotu zamówienia w sposób mogący utrudniać uczciwą konkurencję z uwagi na wymaganie, aby:

a) Zaoferowany system SIEM był zakwalifikowany w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert) lub w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert), podczas gdy są systemy SIEM spełniające wymagania Zamawiającego, znajdujące się w innych opracowaniach badawczych, co nie jest uzasadnione obiektywnymi potrzebami Zamawiającego, a jednocześnie może utrudniać uczciwą konkurencję, co stanowi naruszenie art. 99 ust. 4 Pzp

b) Dopuszczenie jedynie rozwiązania, które odrębnie zapewnia funkcjonalności SIEM i SOAR z uwagi na konieczność dokonania odrębnej wyceny każdej z tych funkcjonalności w Formularzu Ofertowym (SIEM i SOAR), co uniemożliwia zaoferowanie rozwiązań, zapewniających te dwie funkcjonalności łącznie, pomimo, iż oferują one Zamawiającemu te same możliwości, co nie jest uzasadnione obiektywnymi potrzebami Zamawiającego, a jednocześnie może utrudniać uczciwą konkurencję, co stanowi naruszenie art. 99 ust. 4 Pzp.

Odwołujący2 wniósł o uwzględnienie odwołania i nakazanie zamawiającemu:

1. Usunięcie wymagania, aby system SIEM spełniał wymogi bezpieczeństwa Common Criteria for IT Security Evaluation – Roz. 1 pkt 4 OPZ
2. Usunięcie wymagania złożenia przedmiotowego środka dowodowego w postaci certyfikatu Common Criteria for IT Security Evaluation dla systemu SIEM – Roz. IX pkt 2.1.1. SWZ
3. Zmianę wymagania Roz. 1 pkt 1 OPZ dla systemu SIEM w następujący sposób:*„System SIEM musi być dojrzałym, uznanym na rynku produktem – jako potwierdzenie spełnienia wymagania uznane będzie:*
*a) zakwalifikowanie oferowanego Systemu SIEM w niezależnym najnowszym opracowaniu komercyjnej firmy badawczej dotyczącym rozwiązań klasy SIEM w obszarze liderów*
*lub*
*b) ocena oferowanego systemu SIEM jako "Customers' Choice" w raporcie „2023 Gartner's 'Voice of the Customer' for SIEM"";*
4. Zmianę formularza ofertowego w taki sposób, aby możliwe było zaoferowanie rozwiązania, w którym SOAR nie jest dodatkowo płatny (jest częścią rozwiązania SIEM) np. poprzez dodanie alternatywnej tabeli, umożliwiającej podanie ceny za system, który obie funkcjonalności oferuje w ramach jednej licencji.

Odwołujący wskazał, że posiada interes w uzyskaniu zamówienia oraz może ponieść szkodę na skutek naruszenia przepisów ustawy przez Zamawiającego. Sporządzenie przez Zamawiającego opisu przedmiotu zamówienia w sposób nieuwzględniający wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty oraz w sposób mogący utrudniać uczciwą konkurencję uniemożliwia Odwołującemu złożenie oferty i uzyskanie przedmiotowego zamówienia. Uwzględnienie odwołania doprowadzi do tego, że opis przedmiotu zamówienia będzie zgodny z ustawą, co pozwoli Odwołującemu2 złożyć ofertę i uzyskać zamówienie w Postępowaniu.

W uzasadnieniu zarzutów 1 i 2 Odwołujący2 wskazał, że dokonanie opisu przedmiotu zamówienia jest jedną z najistotniejszych czynności w toku postępowania o udzielenie zamówienia publicznego wywierającą wpływ na niemalże wszystkie czynności dokonywane przez Zamawiającego w toku całego postępowania. Jednymi z podstawowych zasad, którymi musi się kierować Zamawiający sporządzając opis przedmiotu zamówienia są jednoznaczność oraz wyczerpujący charakter opisu przedmiotu zamówienia, a także uwzględnienie wszystkich okoliczności mogących mieć wpływ na sporządzenie oferty.

Zarówno w doktrynie, jak i w orzecznictwie panuje zgodność zarówno, co do tego, jak istotną czynnością jest sporządzenie opisu przedmiotu zamówienia, jak i co do tego, że opis przedmiotu zamówienia powinien umożliwiać wykonawcy bez żadnych wątpliwości i dodatkowych interpretacji ustalić co musi zaoferować oraz jakie są wymagania Zamawiającego.

Opis przedmiotu zamówienia powinien zostać dokonany w sposób jednoznaczny, ma wskazać wykonawcom rzeczywisty zakres zamówienia przy użyciu przejrzystych określeń, nie może pominąć żadnych informacji mających wpływ na sporządzenie oferty (tak: B. Artymowicz i in. [w:] Prawo zamówień publicznych. Komentarz, red. H. Nowak i M. Winiarz, UZP, Warszawa 2021, s. 339). Podobne stanowisko prezentuje M. Stachowiak, stwierdzając, że „Podstawowym obowiązkiem zamawiającego jest dokonanie opisu w sposób jednoznaczny i wyczerpujący, a więc taki, który zapewnia, że wykonawcy będą w stanie, bez dokonywania dodatkowych interpretacji, stwierdzić, co jest przedmiotem zamówienia (jakie usługi, dostawy czy roboty budowlane), oraz że wszystkie elementy istotne dla wykonania zamówienia będą w opisie uwzględnione. Opis przedmiotu zamówienia powinien pozwolić wykonawcom na przygotowanie oferty i obliczenie ceny z uwzględnieniem wszystkich czynników wpływających na nią. Ustawa podaje także, że opisu należy dokonać za pomocą dostatecznie dokładnych i zrozumiałych określeń oraz uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty" (M. Stachowiak [w:] W. Dzierżanowski, Ł. Jaźwiński, J. Jerzykowski, M. Kittel, M. Stachowiak, Prawo zamówień publicznych. Komentarz, Warszawa 2021, art. 99.). Zamawiający nie spełnił tych wymagań formułując OPZ w przedmiotowym postępowaniu.

W przedmiotowym postępowaniu Zamawiający w ocenie Odwołującego2 nie uwzględnił wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty. W załączniku nr 2 – OPZ Rozdz. 1 pkt 4. – do Specyfikacji Warunków Zamówienia, Zamawiający wskazuje, że system SIEM musi spełniać wymogi bezpieczeństwa Common Criteria for IT Security Evaluation potwierdzone certyfikatem wydanym nie wcześniej niż w 2020 roku przez akredytowane laboratorium Common Criteria. Certyfikaty Common Criteria są to międzynarodowe certyfikaty, które potwierdzają, że produkty lub systemy informatyczne spełniają określone wymagania bezpieczeństwa. Certyfikaty te są oparte na normie ISO/IEC 15408, która określa kryteria oceny bezpieczeństwa IT. Certyfikacja konkretnego rozwiązania jest procesem długotrwałym, wymaga przygotowania obszernej dokumentacji oraz wykonania szeregu testów i analiz. Proces certyfikacji trwa na świecie średnio około roku.

Odwołujący2 podkreślił, że certyfikat Common Criteria jest wydawany tylko dla konkretnej wersji produktu (np. jeśli certyfikowano produkt w wersji v1.0, uaktualniona wersja v1.0.1 nie posiada statusu produktu certyfikowanego).

Obecnie tylko jeden producent systemów klasy SIEM (firma IBM) posiada ważny certyfikat Common Criteria wydany dla swojej najnowszej wersji produktu SIEM (Qradar Security Intelligence Platform). Wersja ta ukazała się w

styczniu 2022 r., natomiast certyfikację uzyskała w lipcu 2023 r. – oznacza to, że od momentu jej ukazania się wersja ta nie posiadała certyfikatu przez około 1,5 roku.

Inny producent systemów klasy SIEM, firma SPLUNK, nigdy nie uzyskał certyfikatu Common Criteria dla swojego systemu SIEM (Splunk Enterprise Security). Certyfikat taki posiada jedynie inny produkt tego producenta, tj. Splunk Enterprise, który nie jest systemem klasy SIEM, a jedynie systemem zarządzania logami - przy czym certyfikat ten, nie jest wydany dla najnowszej oferowanej wersji produktu.

Odwołujący2 zaznaczył, że w obszarze systemów SIEM trwa ciągła ewaluacja rozwiązań – producenci nieustannie rozbudowują swoje oprogramowanie dostosowując je do potrzeb rynkowych oraz zmieniających się wektorów ataku (dołączają np. systemy SOAR , systemy UEBA, systemy AI, modyfikują i ulepszają architekturę). Należy zwrócić uwagę, że w ciągu roku producenci wydają często 2, a nawet 4 nowe wersje konkretnego rozwiązania, kolejne poprawki bezpieczeństwa czy dodatkowe funkcjonalności. Te ciągłe zmiany w połączeniu z długością procesu certyfikacji powodują, że nie ma możliwości, aby najnowsza dostępna wersja systemu od momentu jej ukazania się posiadała aktualny certyfikat. Wynika to z tego, że istnieje konieczność przeprowadzenia ponownej certyfikacji w przypadku gdy dana wersja produktu ulega zmianie - certyfikat Common Criteria jest wydawany tylko dla konkretnej wersji produktu (np. jeśli certyfikowano produkt w wersji v1.0, uaktualniona wersja v1.0.1 nie posiada statusu produktu certyfikowanego). Odwołujący2 wskazał, że więcej szczegółów można przeczytać na stronie https://commoncriteriaportal.org lub stronie Jednostki Certyfikującej NASK https://www.nask.pl/pl/dzialalnosc/certyfikacja/3858,Certyfikacja.html

W dokumencie „Informator dla Klientów Jednostki Certyfikującej NASK Certyfikat Common Criteria na zasadach określonych przez: Program oceny i certyfikacji bezpieczeństwa IT", w Rozdziale 13 znajduje się informacja dotycząca czasu trwania procesu certyfikacji: „Proces oceny i certyfikacji trwa na świecie średnio około roku. Czas trwania zależy od wielu czynników, z których najważniejszymi są złożoność produktu podlegającego ocenie i deklarowany poziom uzasadnienia zaufania (EAL). Przeprowadzenie oceny wiąże się z przygotowaniem produktu (zgodnie ze standardem CC), przygotowaniem niezbędnej dokumentacji, przekazaniem do ewaluacji akredytowanemu Laboratorium oraz oceny zgodności i wydaniem ostatecznego certyfikatu przez akredytowaną Jednostkę Certyfikującą".

Dodatkowo w tym samym dokumencie w Rozdziale 14 znajduje się wyjaśnienie dotyczące konieczności przeprowadzenia ponownej certyfikacji w przypadku kiedy dana wersja produktu ulega zmianom: „Certyfikat standardu Common Criteria dotyczy produktu w konfiguracji i wersji zadeklarowanej w danej Specyfikacji Zabezpieczeń (ST). Dla przykładu, jeśli certyfikowano produkt w wersji v1.0, uaktualniona wersja v1.0.1 nie posiada statusu produktu certyfikowanego. W przypadku nieznacznych zmian produktu certyfikowanego dostępna jest uproszczona ścieżka służąca uaktualnieniu certyfikatu, zwana Utrzymaniem Zaufania (AC – Assurance Continuity)".

Zgodnie z treścią Załącznika nr 2 – OPZ Rozdz. 1. pkt 18, Zamawiający oczekuje, że: „Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM i Systemu SOAR na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania" oraz w pkt 17, że: „System SIEM i System SOAR muszą być objęte wsparciem technicznym Producenta przez cały okres na jaki zostały kupione licencje. Wsparcie to w szczególności musi pozwalać na nieodpłatne instalowanie wszelkich poprawek, aktualizacji i najnowszych wersji Oprogramowania".

Jak wskazano wyżej, obecnie tylko jeden z producentów rozwiązań klasy SIEM posiada certyfikat Common Criteria dla najnowszej wersji swojego produktu. Biorąc pod uwagę, że w trakcie trwania postępowania producent może wprowadzić na rynek nowszą wersję oprogramowania oraz długi czas na uzyskanie certyfikacji dla tej wersji wymaganie to jest niemożliwe do spełnienia przez wykonawcę.

Oznacza to, że Zamawiający określił wymagania dla systemu SIEM w ten sposób, że wymaga od wykonawcy realizacji świadczenia niemożliwego – dostarczenia systemu spełniającego wymagania Common Criteria for IT Security Evaluation, których potwierdzenie jest niemożliwe dla najnowszej wersji oprogramowania SIEM z uwagi na czas certyfikacji Common Criteria i częstotliwość publikacji nowych wersji oprogramowania. Certyfikacja zajmuje około roku a aktualizacje są publikowane przez producentów oprogramowania nawet do czterech razy na rok.

W konsekwencji również wymaganie, aby wykonawca złożył certyfikaty Common Criteria for IT Security Evaluation jako przedmiotowe środki dowodowe dla oferowanych systemów SIEM i SOAR należy uznać za nieproporcjonalne. Z uwagi na procedurę ich wystawiania nie są one adekwatne do potwierdzenia spełniania przez oferowane dostawy wymagań określonych przez Zamawiającego – najnowsza wersja systemu SIEM nie może być objęta certyfikatem Common Criteria z uwagi na to, że każda zmiana wersji wymaga kolejnej certyfikacji, która z kolei trwa dłużej niż okres pomiędzy aktualizacjami oprogramowania.

W zakresie zarzutów opisanych w pkt 3 odwołania Odwołujący2 podkreślił, że swoboda Zamawiającego w sporządzaniu opisu przedmiotu zamówienia nie jest nieograniczona. Zgodnie z art. 99 ust. 4 ustawy „Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów.".

W doktrynie można spotkać się ze stanowiskiem, że „Cel regulacji z art. 99 ust. 4 Pzp można zdefiniować, posługując się motywem 74 preambuły dyrektywy klasycznej, gdzie wskazano, że „specyfikacje techniczne [opis przedmiotu zamówienia] powinny być opracowywane w taki sposób, aby uniknąć sztucznego zawężania konkurencji poprzez wymogi, które faworyzują konkretnego wykonawcę, odzwierciedlając kluczowe cechy dostaw, usług lub robót budowlanych oferowanych zwykle przez tego wykonawcę". Zasadniczo każdy opis przedmiotu zamówienia oddziałuje na konkurencję. Dyrektywa klasyczna w motywie 74 preambuły dostrzega tę okoliczność, stwierdzając, że niedopuszczalne jest zawężenie, które ma charakter „sztuczny", tzn. faworyzuje (lub dyskryminuje) określonego wykonawcę lub produkt. Niedopuszczalne jest zatem w świetle art. 99 ust. 4 Pzp zaburzenie konkurencji pomiędzy wykonawcami, mające swoją genezę w przygotowanym opisie przedmiotu zamówienia, polegające albo na preferencji w opisie konkretnego wykonawcy lub produktu, albo na niemającym uzasadnieniu wyeliminowaniu wykonawcy lub produktu. Poprzez niedopuszczalne preferowanie należy rozumieć wszystkie zabiegi, przy użyciu dowolnych sposobów opisu przedmiotu zamówienia, które w sposób nieuzasadniony preferują lub wprost wskazują na konkretnego wykonawcę lub konkretny produkt. Skutkiem takiego zapisu jest niemożność złożenia oferty zgodnej z tak sformułowanym opisem przedmiotu zamówienia przez wykonawcę innego niż preferowany lub zaproponowania innego niż preferowany produkt." (tak: Prawo zamówień publicznych. Komentarz, red. H. Nowak i M. Winiarz, B. Artymowicz i in., UZP, Warszawa 2021, s. 340). Podobnie M. Stachowiak stwierdza, że „zamawiający ma ograniczoną swobodę precyzowania wymagań, w tym sensie, że muszą one mieć uzasadnienie; osiągnięcie określonego celu uzasadnionego potrzebami zamawiającego jest przeciwwagą dla ograniczenia konkurencji. Sąd Okręgowy w Poznaniu w wyroku z 11.08.2006 r., IX Ga 137/06, niepubl., rozpatrując granice swobody opisu przedmiotu zamówienia, podkreślił: „Prawo zamówień publicznych chroni bowiem z jednej strony interes Zamawiającego (interes publiczny), z drugiej nakazuje przestrzegać zasady równego traktowania potencjalnych wykonawców i uczciwej konkurencji. Formułując SIWZ, Zamawiający musi mieć na uwadze dobra chronione tą ustawą i

zachować równowagę pomiędzy rozwiązaniami preferującymi poszczególne interesy". Ograniczeniem konkurencji będzie dokonywanie opisu w sposób wskazujący na jeden produkt, usługę lub wykonawcę lub też opisanie przedmiotu zamówienia zbyt szczegółowo, nie pozostawiając miejsca dla przedstawienia ofert zróżnicowanych co do świadczenia, bez uzasadnienia potrzebami zamawiającego (za: M. Stachowiak [w:] W. Dzierżanowski, Ł. Jaźwiński, J. Jerzykowski, M. Kittel, M. Stachowiak, Prawo zamówień publicznych. Komentarz, Warszawa 2021, art. 99.). Opis przedmiotu zamówienia w przedmiotowym postępowaniu, został dokonany w sposób faworyzujący wykonawców obecnie świadczących usługi na rzecz Zamawiającego i utrudniający (uniemożliwiający) złożenie ofert innym wykonawcom.

Zamawiający w przedmiotowym postępowaniu opisał przedmiot zamówienia w sposób ograniczający możliwość oferowania różnych rozwiązań, które to ograniczenia nie są uzasadnione jego obiektywnymi potrzebami.

Przechodząc do zarzutu opisanego w pkt 3a odwołania Odwołujący2 wskazał, że w załączniku nr 2 – OPZ Rozdz. 1 pkt 1. – do Specyfikacji Warunków Zamówienia, Zamawiający wskazuje, że system SIEM musi być dojrzałym, uznanym na rynku produktem, a na potwierdzenie tego wymaga:

1.1. zakwalifikowania oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert)

lub

1.2. zakwalifikowania oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert).

Po pierwsze należy zauważyć, że zarówno Gartner jak i Forrester Reserach Inc. nie są jedynymi niezależnymi, liczącymi się na rynku światowym firmami badawczymi analizującymi rozwiązania klasy SIEM. Można tu wymienić inne firmy badawcze takie jak np. GigaOM, KuppingerCole, czy SC Media.

Po drugie wymaganie Zamawiającego wskazuje na konkretny rodzaj raportu obu firm.

Tymczasem firmy te przygotowują różne rodzaje raportów – są to raporty będące wynikiem pracy zatrudnionych przez nich analityków oraz raporty bazujące na doświadczeniach klientów użytkujących różne rozwiązania SIEM.

Jednym z raportów bazujących na doświadczeniach klientów, jest publikowany przez firmę badawczą Gartner raport "2023 Gartner's 'Voice of the Customer for SIEM". Jest to raport oparty na zweryfikowanych przez Gartner opiniach klientów o dostawcach SIEM. Raport ten dostarcza zagregowaną perspektywę porównawczą na temat rozwiązań, w tym ich mocnych i słabych stron, oraz ogólnego zadowolenia klientów. Raport zawiera również oceny klientów dotyczące możliwości produktu, doświadczenia sprzedażowego, doświadczenia wdrożeniowego i doświadczenia w zakresie wsparcia technicznego producenta.

Raport ten zawiera zatem ocenę systemu SIEM wydaną przez samych klientów, którzy używają danej technologii przyznając kategorię "Customers' Choice" tym rozwiązaniom które zostały docenione przez samych użytkowników. Więcej szczegółów znajduje się na stronie:

https://www.gartner.com/reviews/market/security-information-event-management

W konsekwencji wymaganie, aby oferowany system SIEM był zakwalifikowany jedynie w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów lub w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów, należy uznać za nieuzasadnione obiektywnymi potrzebami Zamawiającego ograniczenie uczciwej konkurencji w Postępowaniu, gdyż istnieją systemy SIEM spełniające wymagania Zamawiającego, które zostały zakwalifikowane do raportów innych firm badawczych lub raportów stworzonych w oparciu o oceny podmiotów użytkujących systemy SIEM.

Ograniczenie opracowań firm badawczych, do których muszą się kwalifikować oferowane systemy SIEM w sposób sztuczny ogranicza zakres możliwych do zaoferowania systemów, niezależnie od tego, czy oferowane systemy spełniają wymagania Zamawiającego. Uzależnienie możliwości zaoferowania danego systemu SIEM od uwzględnienia tego rozwiązania w konkretnym raporcie konkretnej firmy nie wynika z obiektywnych potrzeb Zamawiającego wyrażonych w dokumentach zamówienia.

W odniesieniu do zarzutu 3b odwołania Odwołujący2 podniósł, iż w załączniku nr 1 – Formularz ofertowy – do Specyfikacji Warunków Zamówienia, Zamawiający przedstawił Tabelę nr 1, w której wykonawca powinien podać oddzielną cenę dla Systemu SIEM oraz dla Systemu SOAR [kol. a]. Zamawiający oczekując takiej prezentacji oferty nie dopuścił sytuacji, w której wykonawca mógłby dostarczyć rozwiązanie, w którym SOAR jest integralną częścią Systemu SIEM i nie jest oddzielenie wyceniany. Tym samym Zamawiający dopuszcza jedynie rozwiązania, które są płatne oddzielnie, nie dopuszczając rozwiązań, które spełniają wymagania Zamawiającego dla SIEM i SOAR opisane w Załączniku nr 2 – OPZ w ramach tej samej licencji.

Takie ograniczenie utrudnia uczciwą konkurencję poprzez wyłączenie możliwości zaoferowania systemów, które pozwoliłyby Zamawiającemu uzyskać oczekiwane przez niego funkcjonalności w ramach jednej licencji. Nie znajduje to oparcia w obiektywnie uzasadnionych potrzebach Zamawiającego i w sztuczny sposób ogranicza możliwość zaoferowania rozwiązań, które łącznie zapewniają funkcjonalności SIEM i SOAR oraz preferuje te produkty, w których obydwie te funkcjonalności są zapewniane przez oddzielne systemy.

To, czy Zamawiający otrzyma narzędzie SOAR wbudowane w system SIEM, które będzie spełniało wszystkie wymagania określone przez Zamawiającego, czy też dwa odrębne systemy SIEM i SOAR, nie ma znaczenia z punktu widzenia realizacji potrzeb Zamawiającego. W konsekwencji wyłączenie możliwości zaoferowania systemu SIEM z funkcjonalnością SOAR w ramach jednej licencji należy uznać za nieuzasadnione obiektywnymi potrzebami Zamawiającego ograniczenie uczciwej konkurencji.

Wykonawca wskazuje, że na brak znaczenia po stronie Zamawiającego tego, czy zostanie zaoferowane jedno rozwiązanie obejmujące łącznie funkcjonalności SIEM i SOAR, czy też dwa odrębne systemy wskazuje również to, że cenom za poszczególne funkcjonalności (cena za System SIEM oraz cena za System SOAR) nie przypisano odrębnych kryteriów oceny oferty, natomiast ocenie podlegają, łączna wartość brutto złożonej oferty oraz pozostałe parametry funkcjonalne.

Przystąpienie do postępowania odwoławczego o sygn. akt KIO 3427/23 po stronie odwołującego zgłosił wykonawca FINTECH spółka akcyjna z siedzibą w Warszawie.

Przystąpienie do postępowania odwoławczego o sygn. akt 3427/23 po stronie zamawiającego zgłosił wykonawca PASSUS spółka akcyjna z siedzibą w Warszawie.

W dniu 28 listopada 2023 r. Zamawiający złożył do akt sprawy odpowiedź na odwołanie, w ramach której wnosił o oddalenie odwołania o sygn. akt KIO 3399/23 w całości i przywołał argumentację na poparcie swojego stanowiska, w tym w szczególności treść modyfikacji dokumentów zamówienia, której dokonano w dniu 27.11.2023 r.

***Na podstawie dokumentacji przedmiotowego postępowania, złożonych dowodów oraz biorąc pod uwagę stanowiska stron i uczestników postępowania odwoławczego, Izba ustaliła i zważyła, co następuje:***

Izba stwierdziła, że nie została wypełniona żadna z przesłanek skutkujących odrzuceniem któregokolwiek z odwołań na podstawie art. 528 Pzp i skierowała oba odwołania na rozprawę.

Izba uznała, że odwołujący w obu sprawach posiadali interes w uzyskaniu zamówienia oraz mogli ponieść szkodę w wyniku naruszenia przez zamawiającego przepisów ustawy, czym wypełnili materialnoprawne przesłanki dopuszczalności odwołań, o których mowa w art. 505 ust. 1 Pzp.

Wobec spełnienia przesłanek określonych w art. 525 Pzp, Izba stwierdziła skuteczność zgłoszonych przystąpień przez:
- wykonawcę PASSUS spółka akcyjna z siedzibą w Warszawie (zwanego dalej nadal jako: „przystępujący PASSUS"), do udziału w postępowaniu odwoławczym po stronie zamawiającego w obu sprawach;
- wykonawcę FINTECH spółka akcyjna z siedzibą w Warszawie (zwanego dalej jako: „przystępujący FINTECH"), do udziału w postępowaniu odwoławczym po stronie Odwołującego2 w sprawie o sygn. akt KIO 3427/23.
W związku z tym ww. wykonawcy stali się uczestnikami postępowania odwoławczego.

Na posiedzeniu niejawnym z udziałem stron i uczestników dokonał czynności formalnoprawnych i sprawdzających w zakresie obejmującym okoliczność, że w dniu 27 listopada 2023 r. dokonał modyfikacji postanowień dokumentów zamówienia, które dotyczyły także postanowień objętych odwołaniami. W przypadku postanowień dotyczących sprawy o sygn. akt KIO 3399/23 modyfikacje dotyczyły m.in. postanowień:
- pkt 1 ppkt 5 SOPZ poprzez jego usunięcie;
- pkt 1 ppkt 6 SOPZ poprzez jego usunięcie;
- pkt 1 ppkt 16 SOPZ poprzez nadanie mu brzmienia: „*System SIEM musi posiadać wbudowane mechanizmy kompresji danych przetwarzanych online na zasobach dyskowych na poziomie minimum 30% w stosunku do wielkości otrzymywanych danych lub ograniczania ilości danych przetwarzanych online przed rozpoczęciem ich przetwarzania za pomocą filtracji lub selekcji danych na urządzeniach kolekcjonujących zdarzenia*."
- pkt 2 ppkt 19 SOPZ poprzez jego usunięcie;
- pkt 6 ppkt 22 SOPZ poprzez jego usunięcie;
- pkt 8 ppkt 1 SOPZ poprzez jego usunięcie;
- pkt 8 ppkt 6 SOPZ poprzez nadanie mu brzmienia:„*System SOAR musi zapewniać możliwość kontroli wersji dostępnych scenariuszy (playbooks) w postaci automatycznego lub ręcznego wersjonowania*."

W ocenie Izby, w świetle powyższego oraz treści odwołania w sprawie o sygn. akt KIO 3399/23 nie budzi wątpliwości, iż w przedmiotowej sprawie, w związku z dokonanymi zmianami SWZ może znaleźć zastosowanie art. 568 pkt 2 ustawy Pzp, zgodnie z którym Izba umarza postępowanie odwoławcze w przypadku stwierdzenia, że dalsze postępowanie stało się z innej przyczyny zbędne. Zamawiający po wniesieniu odwołania KIO 3399/23dokonał zmiany postanowień SWZ, do których odnosiły się zarzuty odwołania poprzez usunięcie niektórych z nich lub ich zmianę poprzez nadanie im brzmienia w całości zgodnego z oczekiwanym przez Odwołującego1. Zmiany te nie zostały przez Zamawiającego jedynie zasygnalizowane, ale zostały jednoznacznie do dokumentów postępowania wprowadzone i opublikowane w odpowiednim publikatorze.

Dostrzeżenia wymaga, iż zgodnie z treścią art. 552 ust. 1 Pzp Izba wydając orzeczenie bierze pod uwagę stan rzeczy ustalony na moment zamknięcia postępowania odwoławczego. Ustawodawca przewidział zatem sytuację, w której może dojść do zmian w toku postępowania o udzielenie zamówienia – co Izba zobowiązana jest uwzględnić wydając orzeczenie w sprawie w toku postępowania przed Izbą. Zauważenia również wymaga, że przepisy Pzp nie zobowiązują Zamawiającego do zawieszenia postępowania o udzielenie zamówienia, wobec wniesionego odwołania.
Izba wskazuje, że treść art. 552 ust. 1 ustawy Pzp, podobnie jak w przypadku art. 316 § 1 kpc, w myśl którego podstawą wydania przez sąd wyroku jest stan rzeczy istniejący
w chwili zamknięcia rozprawy – nakazuje uwzględnienie aktualnego stanu faktycznego
w postępowaniu o udzielenie zamówienia. Ponadto stan rzeczy - o którym mowa jest
w przepisie art. 552 ust. 1 ustawy Pzp - należy analogicznie - jak w art. 316 § 1 kpc - interpretować jako okoliczności faktyczne ustalone przed zamknięciem rozprawy oraz stan prawny, tj. obowiązujące przepisy, które mogą stanowić podstawę rozstrzygnięcia
(wyrok SN z 25.06.2015 r., sygn. akt: V CSK 535/14, wyrok Sądu Apelacyjnego ze Szczecina z 13.09.2018 r., sygn. akt: I Aga 159/18).
Rolą ustalenia stanu rzeczy na moment zamknięcia postępowania odwoławczego jest uwzględnienie aktualnego stanu faktycznego w postępowaniu o udzielenie zamówienia. Izba jest więc w takim przypadku zobowiązania uwzględnić czynności Zamawiającego, które miały miejsce po wniesieniu odwołania, do czasu wydania orzeczenia w sprawie. Skoro Zamawiający dokonał czynności zmiany postanowień SWZ odnoszących się do punktów będących podstawą wniesienia odwołania w ten sposób, że usunął postanowienia SWZ, do których odnosiły się zarzuty ww. odwołania i których prawidłowość kwestionował Odwołujący1, bądź też nadał im treść odpowiadającą literalnie treści żądania sformułowanego w odwołaniu, uznać w takiej sytuacji w ocenie składu orzekającego Izby należy, iż w zakresie tych postanowień prowadzenie dalszego postępowania odwoławczego jest bezcelowe, czyli jak stanowi przepis ustawy Pzp – zbędne.

W konsekwencji mając na względzie okoliczności niniejszej sprawy, orzeczono jak
w sentencji, na podstawie przepisu art. 568 pkt 2 ustawy Pzp, umarzając w części postępowanie odwoławcze.
Izba zaliczyła na poczet materiału dowodowego:

1)dokumentację przekazaną w obu sprawach w postaci elektronicznej, zapisaną na płycie DVD, przesłaną do akt sprawy przez zamawiającego w dniu 22 listopada 2023 r., w tym w szczególności:
- specyfikację warunków zamówienia (zwaną dalej nadal: „SWZ");
- Formularz ofertowy, stanowiący załącznik nr 1 do SWZ;
- Szczegółowy Opis Przedmiotu Zamówienia (dalej „SOPZ"), stanowiący załącznik nr 2 do SWZ;
2)dokumenty złożone na posiedzeniu przez Odwołującego1 w sprawie o sygn. akt KIO 3399/23: - tłumaczenie opracowania Magic Quadrant dla Systemów Zarządzania Informacjami Bezpieczeństwa i Zdarzeń (SIEM) oraz
- tłumaczenie opracowania The Forrester Wave: Security Analytics Platform, Q4 2022;
3)dokumenty złożone na posiedzeniu przez Odwołującego2 w sprawie o sygn. akt KIO 3427/23:
- wyciąg z dokumentu Informator dla Klientów Jednostki Certyfikującej NASK – Certyfikat Common Criteria na zasadach określonych przez: Program oceny i certyfikacji bezpieczeństwa IT;
- wycinki ze strony internetowej: https://www.commoncriteriaportal.org/products/index.cfm z dnia 28.11.2023 r. wraz z tłumaczeniem oraz wycinek ze strony internetowej https://www.ibm.com/community/qradar/home/software z dnia

27.11.2023 r. wraz z tłumaczeniem
- wycinek ze strony internetowej https://www.splunk.com z dnia 27.11.2023 r. wraz z tłumaczeniem;
- zestawienie ofert złożonych w postępowaniu prowadzonym przez Zamawiającego w roku 2021 r. pn. *Umowa ramowa na dostawę rozwiązania informatycznego obejmującego funkcjonalność systemu zarządzania informacją i zdarzeniami bezpieczeństwa SIEM/SOAR oraz świadczenie innych usług;*
- wycinek ze strony internetowej: https://www.gigaom.com/reprint/gigaom-radar-for-security-information-and-event-management-siem-224222-sumologic/ z dnia 27.11.2023 r. wraz z tłumaczeniem;
- wycinek ze strony internetowej: https://www.kuppingercole.com/research/lc80473/intelligent-siem-platforms z dnia 27.11.2023 r. wraz z tłumaczeniem
- wycinek ze strony internetowej: https://www.gartner.com/doc/reprints?id=1-2D5GUAI3&ct=230405&st=sb z dnia 27.11.2023 r. wraz z tłumaczeniem;
- wyciąg z raportu Gartner Magic Quadrant for Security Information and Event Management 2022 (10 October 2022 – ID G00755317) wraz z tłumaczeniem

4)dokumenty złożone przez Zamawiającego w toku rozprawy w zakresie sprawy o sygn. akt KIO 3399/23 tj.:
- wycinek ze strony internetowej: https://sodan.io
- wyciągi z publikacji NIST tj. amerykańskiego regulatora w zakresie ochrony cyberprzestrzeni wraz z tłumaczeniem

Izba postanowiła oddalić wniosek dowodowy złożony w toku rozprawy przez Odwołującego1 obejmujący przeprowadzenie dowodu z opinii biegłego - opinii NASK – Państwowego Instytutu Badawczego.Skład orzekający miał na uwadze, że zgodnie z art. 531 Pzp „przedmiotem dowodu są fakty mające dla rozstrzygnięcia sprawy istotne znaczenie". Ponadto, zważywszy na treść art. 539 ust. 2 Pzp należy stwierdzić, że dowód z opinii biegłego można przeprowadzić w przypadku, gdy ustalenie stanu faktycznego sprawy wymaga wiadomości specjalnych. Z treści wniosku o przeprowadzenie tego dowodu wynika zaś, że przedmiotem dowodu nie miałoby być ustalenie faktów wymagające wiadomości specjalnych, lecz ocena czy wymagania określone w określonych punktach SOPZ są uzasadnione interesem Zamawiającego oraz czy potrzeby określone przez Zamawiającego mogą być zapewnione w sposób inny niż opisany w SOPZ, a tym samym biegły miałby w praktyce dokonać oceny działalności Zamawiającego w zakresie sformułowanych przez niego potrzeb oraz przyjętego sposobu ich realizacji, co w świetle ww. przepisów należy uznać za niedopuszczalne.

Izba ustaliła, następujące okoliczności faktyczne jako istotne:

Zamawiający prowadzi postępowanie o udzielenie zamówienia publicznego w celu zawarcia umowy ramowej z odpowiednim stosowaniem przepisów dotyczących trybu przetargu nieograniczonego na podstawie przepisów" pn.: Umowa ramowa na dostawę rozwiązania informatycznego obejmującego funkcjonalność zarządzania informacją i zdarzeniami bezpieczeństwa SIEM/SOAR oraz świadczenie innych usług towarzyszących")", o numerze: WZP-421-16/2023, zwane dalej: „postępowaniem".

Treść przepisów dotyczących zarzutów:

- art. 99 ust. 1 Pzp – *Przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty*;
- art. 99 ust. 4 Pzp – *Przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania*
*lub wyeliminowania niektórych wykonawców lub produktów.*;
- art. 106 ust. 2 Pzp – *Zamawiający żąda przedmiotowych środków dowodowych proporcjonalnych do przedmiotu zamówienia i związanych z przedmiotem zamówienia.*;
- art. 226 ust. 1 pkt 2 lit. a Pzp – *Zamawiający odrzuca ofertę, jeżeli została złożona przez wykonawcę podlegającego wykluczeniu z postępowania*;
- art. 16 pkt 1 Pzp – *Zamawiający przygotowuje i przeprowadza postępowanie o udzielenie zamówienia w sposób:*
*1) zapewniający zachowanie uczciwej konkurencji oraz równe traktowanie wykonawców.*;

Izba zważyła co następuje.

Po zapoznaniu się z argumentacją stron i uczestników postępowań odwoławczych o sygn. akt KIO 3399/23 (Odwołanie1) i sygn. akt KIO 3427/23 (Odwołanie2), wyrażoną w pismach wniesionych w tych postępowaniach oraz przedstawionymi w trakcie rozprawy, Izba uznała, że odwołanie o sygn. akt KIO 3399/23 nie zasługiwało na uwzględnienie, zaś odwołanie o sygn. akt KIO 3427/23 zasługiwało na uwzględnienie w części.

Zawarty w Odwołaniu1 zarzut naruszenia art. 99 ust. 1, 2 i 4 PZP w zw. z art. 16 PZP nie był uzasadniony.

W pierwszej kolejności Izba wskazuje, że z uwagi na zmianę części postanowień Szczegółowego Opisu Przedmiotu Zamówienia, stanowiącego Załącznik nr 2 do Specyfikacji Warunków Zamówienia (dalej: SOPZ), których dotyczyła treść zarzutu podniesionego przez Odwołującego1, postępowanie odwoławcze podlegało częściowemu umorzeniu w zakresie wskazanym w sentencji wyroku.

W zakresie w jakim Odwołujący1 podtrzymał swoje zarzuty, odwołanie podlegało oddaleniu.

Treść Odwołania1 odnosiła się do zapisów Szczegółowego Opisu Przedmiotu Zamówienia (dalej: SOPZ) stanowiącego Załącznik nr 2 do Specyfikacji Warunków Zamówienia, którym Zamawiający, zgodnie ze zmianą z dnia 27.11.2023 r. nadał następujące brzmienie:

I.Pkt. 2 ppkt. 13 SOPZ o treści: *„Oprogramowanie Agenta musi mieć możliwość równoważenia obciążenia (wysyłanych danych) pomiędzy kilka serwerów centralnych rozwiązania działających w klastrze lub niezależnie*"

II.Pkt. 2 ppkt 16 SOPZ o treści: *„Rozwiązanie powinno zapewniać dostępność agentów, udostępnionych przez Producenta rozwiązania, do zbierania zdarzeń z serwerów z systemami operacyjnymi Microsoft Windows, Unix/Linux, lub innych serwerów aplikacyjnych, bez konieczności wnoszenia dodatkowych opłat lub zawierać odpowiedni pakiet licencji, gwarantujący możliwość zainstalowania stosownego agenta na każdym z możliwych do podłączenia źródeł, które Jednostki będą chciały podłączyć do Systemu SIEM*."

*III.*Pkt. 2 ppkt. 18 SOPZ o treści: *„Oprócz źródeł wymienionych wyżej System SIEM musi umożliwiać pobieranie informacji z wykorzystaniem poniższych mechanizmów:*
*18.1 dane wydajnościowe Windows Performance Monitor,*
*18.2 dowolne dane WMI,*
*18.3 wynik działania programów i skryptów uruchamianych na urządzeniu/serwerze lub na podłączonym systemie*

*źródłowym,*
*18.4 Zmiany w zawartości plików i kluczy rejestrów. 1*
*8.5 Pliki tekstowe na zdalnych serwerach poprzez SSH, CIFS i NFS."*

IV.Pkt. 3 ppkt. 3 SOPZ o treści: *„Musi istnieć możliwość wzbogacania danych pochodzących z logów, o informacje zwarte w zewnętrznych repozytoriach: a) Katalogi LDAP, b) Bazy danych, c) Bazy no SQL d) Hadoope) Dane geolokalizacyjne."*

V.Pkt. 4 ppkt. 4 SOPZ o treści:*„Przechowywane dane muszą być zabezpieczone przed modyfikacją z wykorzystaniem metod kryptograficznych (takich jak szyfrowanie danych, podpisy cyfrowe, hashowanie, funkcje skrótu, protokoły bezpiecznej transmisji danych, i inne). Musi być możliwe przechowywanie danych zabezpieczających (skróty/podpisy) poza systemem. Musi być możliwe znakowanie danych czasem."*

VI.Pkt. 5 ppkt. 12 SOPZ o treści:*„System SIEM musi umożliwiać konfigurację klastrów wysokiej dostępności z równoważeniem obciążenia (klastry Active/Active). Musi istnieć możliwość konfiguracji dowolnej liczby węzłów klastra. Równoważenie obciążenia pomiędzy komponentami systemu SIEM nie może wymagać stosowania zewnętrznego rozwiązania je rozkładającego (tzw. loadbalancer) oraz nie może wymagać zakupu żadnej dodatkowej licencji."*

*VII.*Pkt. 6 ppkt. 6 SOPZ o treści *„System SIEM musi zawierać mechanizmy zarządzania incydentami obejmujące co najmniej:*
*6.1 Możliwość automatycznego tworzenia incydentów na podstawie reguł alarmowych,*
*6.2 Możliwość przypisania incydentu do osoby,*
*6.3 Możliwość zmiany statusu i priorytetu incydentu,*
*6.4 Możliwość tworzenia komentarzy,*
*6.5 Możliwość modyfikowania reguł alarmowych i oznaczania alarmów jako fałszywe alarmy.*
*6.6 Możliwość tworzenia wyjątków stałych i czasowych dla reguł i zdarzeń spełniających określone warunki.*
*6.7 Możliwość raportowania wydajności obsługi incydentów."*

*VIII.*Pkt. 6 ppkt. 23 SOPZ o treści: *„System SIEM musi umożliwiać pod warunkiem braku ingerencji w kod źródłowy systemu SIEM i nienaruszania praw autorskich i patentowych, tworzenie własnych, nieprzewidzianych przez producenta funkcjonalności związanych z analizą danych z wykorzystaniem zewnętrznych komponentów komercyjnych obejmujących:*
*23.1 mechanizmy pobierania danych,*
*23.2 raporty, dashboardy i formularze,*
*23.3 nowe funkcje analityczne,*
*23.4 nowe sposoby wizualizacji,*
*23.5 mechanizmy powiadamiania, w tym dwukierunkowe - inne niż przewidział producent. Realizacja tych funkcjonalności przez Jednostki może wymagać konieczności angażowania Producenta i nie może naruszać jego praw autorskich. Komponenty oferowanego rozwiązania nie muszą pochodzić od jednego Producenta, jednak nie mogą być to rozwiązania open source.*

Należy wskazać na wstępie, że zgodnie z art. 99 ust. 1 Pzp przedmiot zamówienia opisuje się w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty, a w ustępie 4 ustawodawca wskazał, że przedmiotu zamówienia nie można opisywać w sposób, który mógłby utrudniać uczciwą konkurencję, w szczególności przez wskazanie znaków towarowych, patentów lub pochodzenia, źródła lub szczególnego procesu, który charakteryzuje produkty lub usługi dostarczane przez konkretnego wykonawcę, jeżeli mogłoby to doprowadzić do uprzywilejowania lub wyeliminowania niektórych wykonawców lub produktów.

Izba podkreśla, że istotą zamówień publicznych jest stworzenie transparentnego, jasnego i przejrzystego modelu gospodarowania środkami publicznymi. Zamawiający w ramach zamówień publicznych nie rozporządzają własnym mieniem, wedle własnych osobistych preferencji czy powiązań, ale mieniem publicznym. Ustawodawca wyraźnie wskazuje, iż takie dysponowanie mieniem publicznymi, środkami publicznymi powinno mieć na celu dążenie do uzyskania zamówienia reprezentującego najlepszy możliwy stosunek jakości do ceny z perspektywy zaspokojenia potrzeb leżących w interesie publicznym (lokalnym). Konieczne jest przy tym zapewnienie, aby przy zaspokajaniu owych potrzeb publicznych zachowana była zasada wolności gospodarczej i możliwości dostępu do wykonywania zadań publicznych na niedyskryminacyjnych warunkach przez przedsiębiorców działających na rynku. Nie ulega również wątpliwości, że zamawiający może dopasować zamówienie do swoich obiektywnych potrzeb, ale te obiektywne potrzeby czy wymagania nie mogą sprowadzać się do określenia parametrów, które wskazują na jeden konkretny produkt. Należy jednak zaznaczyć, że takie potrzeby mogą powodować, że liczba wykonawców zdolnych do wykonania zamówienia będzie ograniczona. Fakt, że na rynku występują wykonawcy nieprodukujący danego przedmiotu zamówienia lub dla których jego realizacja jest utrudniona czy nieopłacalna, nie przesądza wcale o możliwości powstania naruszenia zasady uczciwej konkurencji. Dla stwierdzenia takiego naruszenia niezbędne jest zbadanie i ocena co najmniej kilku okoliczności związanych z danym zamówieniem, w szczególności takich jak kształt rynku, którego zamówienie dotyczy oraz skutków ograniczenia konkurencji dla ilości potencjalnych wykonawców mogących ubiegać się o uzyskanie zamówienia, a z drugiej strony waga potrzeb zamawiającego, których realizacji takie ograniczenie służy.

Uwzględniając powyższe postulaty, Izba stwierdza, że Odwołujący1 nie wykazał zasadności zarzutów wskazanych w odwołaniu. Na wstępie Izba wskazuje, że to treść odwołania oraz wskazane przez wykonawcę okoliczności faktyczne potwierdzające zasadność naruszenia określonych przepisów Pzp i stanowią podstawę do wydania rozstrzygnięcia przez Izbę. To odwołujący dobiera spektrum okoliczności faktycznych, z których wywodzi zasadność naruszenia przepisów ustawy. Nie może być tak, że zasadność zarzutów odwołujący upatruje wyłącznie w oparciu o jednozadaniowe stwierdzenia, że postanowienia SWZ ograniczają konkurencję. Jest oczywistym dla Izby, że możliwość wykazania szeregu okoliczności faktycznych wymaga dużego zaangażowania wykonawcy w procesie badania i analizy wymagań zamawiającego w świetle uwarunkowaniach rynkowych. Jednakże wykonawca jako profesjonalista działający w obszarze w którym ubiega się o zamówienie, w oparciu o swoją profesjonalną wiedzę i doświadczenie zobowiązany jest podjąć inicjatywę dowodową w celu wykazania zasadności swoich twierdzeń. Takie działanie wykonawcy – odwołującego jest skorelowane z art. 534 ust. 1 ustawy – Strony i uczestnicy postępowania odwoławczego są obowiązani wskazywać dowody do stwierdzenia faktów, z których wywodzą skutki prawne. Dowody na poparcie swych twierdzeń lub odparcie twierdzeń strony przeciwnej strony i uczestnicy postępowania odwoławczego mogą przedstawiać aż do zamknięcia rozprawy. Przepis ten nakłada na Strony postępowania obowiązek, który zarazem jest uprawnieniem Stron, wykazywania dowodów na stwierdzenie faktów, z których wywodzą skutki prawne. Postępowanie przed Izbą stanowi postępowanie kontradyktoryjne, czyli sporne, a z istoty tego postępowania wynika, że spór toczą Strony postępowania i to one mają obowiązek wykazywania dowodów, z których wywodzą określone skutki prawne. Powołując w tym miejscu regulację art. 8 Pzp, do czynności podejmowanych przez zamawiającego i wykonawców w postępowaniu o

udzielenie zamówienia publicznego stosuje się przepisy ustawy z dnia 23 kwietnia 1964 roku – Kodeks cywilny, jeżeli przepisy ustawy nie stanowią inaczej. Przechodząc do art. 6 Kodeksu cywilnego ciężar udowodnienia faktu spoczywa na osobie, która z faktu tego wywodzi skutki prawne należy wskazać, iż właśnie z tej zasady wynika reguła art. 534 ust. 1 Pzp. Przepis art. 6 Kodeksu cywilnego wyraża dwie ogólne reguły, a mianowicie wymaganie udowodnienia powoływanego przez stronę faktu, powodującego powstanie określonych skutków prawnych oraz usytuowanie ciężaru dowodu danego faktu po stronie osoby, która z faktu tego wywodzi skutki prawne; ei incubit probatio qui dicit non qui negat (na tym ciąży dowód kto twierdzi a nie na tym kto zaprzecza). Powyższych reguł nie podważa, a wręcz potwierdza je stanowisko orzecznictwa przywoływanego przez Odwołującego1, które każdorazowo nakłada zobowiązanie do uprawdopodobnienia przez wykonawcę możliwości ograniczenia konkurencji przez dokonany przez zamawiającego opis przedmiotu zamówienia.

W analizowanym stanie faktycznym, Odwołujący1 zarzucił Zamawiającemu dokonanie nieprawidłowego opisu przedmiotu zamówienia, wskazując, że zestawienie poszczególnych parametrów wymaganych przez Zamawiającego umożliwia zaoferowanie wyłącznie produktów jednego producenta. W treści Odwołania1 wykonawca nie zawarł jednak żadnej argumentacji, żadnych analiz ani nie powołał się na żadne dowody potwierdzające zasadność swoich twierdzeń. Treść poszczególnych zarzutów Odwołującego sprowadzała się do opisania poszczególnych parametrów kwestionowanych w SWZ oraz wskazania żądanej zmiany. Odwołujący w żaden sposób nawet nie uprawdopodobnił twierdzenia, że zestawienie wymagań Zamawiającego powoduje, iż możliwe jest zaoferowanie urządzeń tylko jednego producenta. Takie okoliczności, zdaniem Izby, Odwołujący1 mógł wykazać, chociażby poprzez przedłożenie na rozprawie lub wraz z odwołaniem zestawienia parametrów technicznych urządzeń dostępnych na rynku. Wykonawcy wielokrotnie właśnie poprzez zestawienie cech technicznych produktów dostępnych na rynku uprawdopodabniają zarzut dotyczący możliwości zaoferowania urządzeń jednego producenta. Odwołujący1 ograniczył się w tym zakresie wyłącznie do złożonego na rozprawie wniosku o przeprowadzenie dowodu z opinii biegłego – instytutu badawczego. Izba wskazuje po pierwsze, że wniosek ten dotyczył wyłącznie trzech z kwestionowanych zapisów SOPZ, po drugie zaś proponowany sposób sformułowania pytań miał na celu ocenę zasadności wskazanych przez Zamawiającego interesów wyrażonych w odpowiedzi na odwołanie, nie zaś kwestii technologicznych poszczególnych rozwiązań funkcjonujących na rynku. Ponadto, Izba podkreśla, że wnioskowany przez Odwołującego1 dowód z opinii biegłego nie może zastępować inicjatywy dowodowej samego wykonawcy. Wykonawca jako profesjonalista formułując zarzuty w odwołaniu winien w pierwszej kolejności uprawdopodobnić ich zasadność, czego zdaniem Izby, Odwołujący1 nie uczynił.

Izba podkreśla również, że zasadnicza treść odwołania sprowadzała się nie do kwestionowania czynności podjętych przez Zamawiającego, lecz do zrecenzowania czy też oceny funkcjonalności jednego z rozwiązań funkcjonujących na rynku, tj. rozwiązania firmy SPLUNK. Ponadto Odwołujący1 podczas rozprawy nie podjął polemiki z szeroko przedstawionym w odpowiedzi na odwołanie stanowiskiem Zamawiającego, pozostając na ograniczonych w treści twierdzeniach, że wymagania postawione przez Zamawiającego są nadmiarowe, gdyż pozostałe rozwiązania systemów SIEM mogą realizować potrzeby Zamawiającego w sposób efektywny oraz ekonomicznie uzasadniony. Izba zaznacza, że to Zamawiający określa swoje potrzeby jakie mają zostać zrealizowane w ramach danego postępowania przetargowego, mając na uwadze istniejące uwarunkowania. Jak wyjaśnił Zamawiający przedmiot zamówienia zostanie przekazany do instytucji wymiaru sprawiedliwości, którzy posiadają już określone zaplecze techniczne, zaś wdrażane szczegółowe rozwiązania mają na celu realizację zadań poszczególnych jednostek. Określając wymagania Zamawiający musiał również wziąć pod uwagę istniejące uwarunkowania oraz dopasowane do struktury systemu zapewnienia bezpieczeństwa cyberbezpieczeństwa budowanego od kilku lat. Zamawiający wyjaśnił również znaczenie parametrów, które zostały zakwestionowane przez Odwołującego w kontekście unifikacji i skalowalności ww. struktury, jej zasadnicze cele i filozofię budowy (m.in. jej uproszczenie poprzez wprowadzenie optymalnego rozwiązania źródło danych – serwery) oraz znaczenie w kontekście prowadzonej ochrony przed cyberatakami lub przestępstwami dot. cyberprzestrzeni.

Odnosząc się do poszczególnych zarzutów, Izba wskazuje co następuje:

1) Możliwość tworzenia własnych funkcjonalności – brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na jednozdaniowym stwierdzeniu, iż udzielane przez komercyjnych producentów licencje na oprogramowanie nie dopuszczają do samodzielnego tworzenia nowych funkcjonalności w ramach ich systemów ze względu na naruszenie praw autorskich i patentowych, bez jakikolwiek analizy i argumentacji.

2) Wprowadzenie do architektury systemu urządzeń typu load-balancer - brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na wskazaniu przez Odwołującego1, że równoważenie obciążenia według najlepszych praktyk jest realizowane na urządzeniach kolekcjonujących dane (centralnych), a nie na agentach zainstalowanych na urządzeniach dostarczających dane, bez jakikolwiek analizy i argumentacji czy dowodów na potwierdzenie twierdzeń. Zamawiający szczegółowo wyjaśnił postawione wymaganie w kontekście uproszczenia budowy struktury poprzez wprowadzenie optymalnego rozwiązania źródło danych – serwery.

3) Możliwość podłączenia niestandardowego źródła danych – brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na jednozdaniowym stwierdzeniu, iż możliwe jest podłączenie niestandardowego źródła danych, jednak musi ono być zweryfikowane na etapie analizy przedwdrożeniowej systemu. Zamawiający wyjaśnił konieczność wymagania oraz doprecyzował wymaganie w zakresie możliwości podłączenia źródeł danych.

4) Protokół SSH - brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na jednozdaniowym stwierdzeniu, iż rozwiązanie nie jest rekomendowane przez ekspertów ds. bezpieczeństwa oraz nie jest to dobra praktyka ze względu na ryzyko wycieku poświadczeń, bez jakikolwiek dalszej analizy i argumentacji.

5) Wprowadzenie plików płaskich CSV - brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na jednozdaniowym stwierdzeniu, że producenci rozwiązań SIEM stosują metody integracji ze tego typu źródłami, najczęściej poprzez normalizację danych do plików płaskich CSV oraz istnieje jedynie wąska grupa producentów SIEM, którzy wykorzystują integrację natywną. Zamawiający wyjaśnił zasadność braku wskazywanego typu plików.

6) Wymóg dodatkowego szyfrowania danych - brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na stwierdzeniu, że dodatkowe wymaganie na szyfrowanie danych wydaje się być nadmiarowe w świetle wymagania dysponowania certyfikatem Common Criteria oraz może ograniczać grupę potencjalnych producentów systemów SIEM, chcących wziąć udział w postępowaniu. Zamawiający wyjaśnił zasadność wymaganej funkcjonalności oraz jej rozumienie.

7) klastry typu Active/Active – stanowisko Odwołującego sprawdzało się do oceny, że żądanie Zamawiającego służy do zapewnienia wysokiej wydajności, a nie wysokiej dostępności, zaś powszechną praktyką adresowania tego typu wymagania jest stosowanie zewnętrznego (sprzętowego lub wirtualnego) load balancer'a na poziomie sieci, bez jakikolwiek analizy i argumentacji czy dowodów na potwierdzenie twierdzeń. Zamawiający szczegółowo wyjaśnił postawione wymaganie w kontekście uproszczenia budowy struktury poprzez wprowadzenie optymalnego rozwiązania źródło danych – serwery.

8) Mechanizm zarządzania incydentami - brak uzasadnienia merytorycznego zarzutu. Zarzut został oparty na stwierdzeniu, iż ograniczenie tego wymagania jedynie do systemu SIEM istotnie ogranicza grupę producentów SIEM, którzy koncentrują się na funkcjonalnościach SIEM, ale zapewniają integrację z szeroką gamą producentów systemów

SOAR, bez jakikolwiek analizy i argumentacji oraz dowodów na potwierdzenie podnoszonych okoliczności.

Tym samym, wobec lakonicznego stanowiska Odwołującego1 wyrażanego w odwołaniu, braku złożenia dowodów, które uprawdopodabniających naruszenie konkurencji, Izba oddaliła odwołanie ww. zakresie.

Zawarty w Odwołaniu2 zarzuty naruszenia art. 99 ust. 1 oraz art. 106 ust. 2 PZP nie były uzasadnione.

Na wstępie wskazania wymaga, że dyspozycja art. 99 Pzp determinuje, aby opis przedmiotu zamówienia został przez zamawiającego sformułowany w sposób jednoznaczny i wyczerpujący, za pomocą dostatecznie dokładnych i zrozumiałych określeń, uwzględniając wszystkie wymagania i okoliczności mogące mieć wpływ na sporządzenie oferty, z zachowaniem zasad uczciwej konkurencji. Zgodnie z orzecznictwem Izby, istota tego przepisu sprowadza się więc do określenia przez zamawiającego swoich wymagań dotyczących przedmiotu zamówienia, tak szczegółowo i tak dokładnie, aby każdy wykonawca był w stanie zidentyfikować, czego zamawiający oczekuje, przy czym zakres obowiązku zamawiającego dotyczącego informacji wymaganych w SWZ jest determinowany przedmiotem zamówienia. Izba podkreśla również, że zarzuty wykonawców względem opisu przedmiotu zamówienia czy zakresu informacji przekazanych przez Zamawiającego w SWZ nie mogą ograniczać się do stwierdzeń, że opis jest niepełny, że nie można wycenić przedmiotu zamówienia, że brakuje bliżej niesprecyzowanych informacji. Korelacją obowiązku zamawiającego jednoznacznego i wyczerpującego opisu przedmiotu zamówienia, jest obowiązek wykonawcy wykazania w sposób jednoznaczny i wyczerpujący jakich konkretnie informacji/dokumentów zamawiający nie przekazał wykonawcom w SWZ, dlaczego są one istotne z punktu widzenia wyceny przedmiotu zamówienia i jakie skonkretyzowane ryzyka występują po stronie wykonawcy z tytuły nieprzekazania takich informacji/dokumentów" (tak też: wyrok KIO z dnia 18 lutego 2021 r., sygn. akt KIO 3045/20, KIO 3143/20).

Izba stwierdziła, że w okolicznościach przedmiotowej sprawy Odwołujący2 nie wykazał, że Zamawiający nie uwzględnił wszystkich wymagań i okoliczności mogących mieć wpływ na sporządzenie oferty prawidłowo, co było treścią postawionego zarzutu.

Treść Odwołania2 w zakresie zarzutu naruszenia art. 99 ust. 1 Pzp odnosiła się do zapisów pkt 1 ppkt 4 Szczegółowego Opisu Przedmiotu Zamówienia (dalej: SOPZ) stanowiącego Załącznik nr 2 do Specyfikacji Warunków Zamówienia, którego brzmienie, zgodnie ze zmianą z dnia 27.11.2023 r. jest następujące:

*System SIEM musi spełniać wymogi bezpieczeństwa Common Criteria for IT Security Evaluation potwierdzone certyfikatem wydanym nie wcześniej niż w 2020 roku przez akredytowane laboratorium Common Criteria. Powyższy wymóg dotyczy systemu (linii produktowej), nie oferowanej, najnowszej wersji systemu wymaganej przez Zamawiającego.*

Ponadto Odwołujący2 przywołał w treści argumentacji pkt 1 ppkt 17 i 18 SOPZ (po zmianach z 27.11.2023 odpowiednio pkt 15 i 16 SOPZ) o następującej treści:

15. *System SIEM i System SOAR muszą być objęte wsparciem technicznym Producenta przez cały okres na jaki zostały kupione licencje. Wsparcie to w szczególności musi pozwalać na nieodpłatne instalowanie wszelkich poprawek, aktualizacji i najnowszych wersji Oprogramowania.*
16. *Wykonawca dostarczy najnowsze wersje Oprogramowania dla Systemu SIEM i Systemu SOAR na dzień dostarczenia licencji, zgodnie z informacjami publikowanymi przez Producenta rozwiązania.*

Z tak sformułowanej treści opisu przedmiotu zamówienia Odwołujący2 wywodził, iż Zamawiający określił w OPZ wymagania dla systemu SIEM w ten sposób, że wymagał od wykonawcy realizacji świadczenia niemożliwego – dostarczenia systemu spełniającego wymagania Common Criteria for IT Security Evaluation, których potwierdzenie jest niemożliwe dla najnowszej wersji oprogramowania SIEM. Takie twierdzenie Odwołującego2 miały potwierdzać okoliczności związane z czasem niezbędnym do dokonania certyfikacji Common Criteria i częstotliwość publikacji nowych wersji oprogramowania.

W pierwszej kolejności należy wskazać, iż twierdzeniom Odwołania2 przeczy zarówno sama treść odwołania, jak również treść dowodu nr 2 przedłożonego przez Odwołującego2. Z treści obu tych dokumentów wynika istnienie na rynku rozwiązań określanych w innym miejscu odwołania jako niemożliwe do zrealizowania.

Niezależnie od powyższego należy zauważyć, że polemika i argumentacja zawarta w odwołaniu w zakresie przedmiotowych zarzutów prowadzona jest z wymogiem opisu przedmiotu zamówienia, którego istnienie kwestionuje Zamawiający, jak również nie wynika ono z treści dokumentów zamówienia.

Zamawiający zarówno w przedłożonej odpowiedzi na odwołanie, jak również w stanowisku przedstawionym na rozprawie konsekwentnie wskazywał, że certyfikat Common Criteria nie jest wymagany dla najnowszej wersji rozwiązania SIEM, zaś wystarczające dla spełnienia wymogów jest, aby dane rozwiązanie SIEM posiadało taki certyfikat dla jakiejkolwiek wersji, wydany nie wcześniej niż przed 2020 r.

Brak istnienia kwestionowanego wymogu potwierdza również treść dokumentacji zamówienia. Należy bowiem zauważyć, że wymóg dysponowania odpowiednim certyfikatem Common Criteria, a także dostarczenia najnowszej wersji oprogramowania zawarte są w dwóch odrębnych punktach SOPZ, które odnoszą się treściowo do odmiennie zdefiniowanych elementów przedmiotu zamówienia. W tym miejscu należy w pierwszej kolejności przywołać treść Rozdziału II pkt 2.14 SWZ, zgodnie z którym*Znaczenie pojęć użytych w SWZ jest tożsame z definicjami przyjętymi we Wzorze Umowy ramowej (Załącznik nr 5 do SWZ) oraz Wzorze umowy wykonawczej (Załącznik nr 5A do SWZ).* Przechodząc z kolei do treści Wzoru Umowy Ramowej, w § 1 ust. 1 zawarto następujące definicje:

*7)System – całość rozwiązania informatycznego obejmującego System SIEM lub System SOAR, zawierającego wszystkie niezbędne elementy w tym wszystkie licencje i Oprogramowanie oraz Sprzęt (o ile dotyczy), umożliwiające realizację funkcjonalności Systemu zgodnie z OPZ, dostarczane Jednostkom;*

*8)System SIEM – (system klasy SIEM - Security Information and Event Management) – rozwiązanie informatyczne służące do zarządzania zdarzeniami i informacjami bezpieczeństwa, z zastrzeżeniem, że rozwiązanie to może stanowić samodzielny przedmiot Umowy wykonawczej;*

*9)System SOAR – (system klasy SOAR - Security Orchestration, Automation And Response) – rozwiązanie służące do automatyzacji i strukturyzacji procesów w systemach informatycznych, z zastrzeżeniem, że rozwiązanie to może stanowić samodzielny przedmiot Umowy wykonawczej;*

*10)Oprogramowanie – całość programów komputerowych, aplikacji oraz wszelkiego pozostałego software'u, w tym oprogramowanie agentów instalowanych na stacjach końcowych oraz usługi zdalnego zarządzania oprogramowaniem agentów wchodzących w skład Systemu, bądź z nim związanych, umożliwiających realizację funkcjonalności Systemu zgodnie z Umową oraz OPZ.*

Z kolei część wstępna SOPZ zawiera następującą treść:

*Przedmiotem zamówienia jest dostawa Systemu składającego się z:*

*a)rozwiązania służącego do zarządzania zdarzeniami i informacjami bezpieczeństwa (system klasy SIEM – Security Information and Event Management) zwanego dalej Systemem SIEM*

*oraz*

*b)rozwiązania służącego do automatyzacji i strukturyzacji procesów w systemach informatycznych (system klasy SOAR - Security Orchestration, Automation And Response) zwanego dalej Systemem SOAR,*

W dalszej części SOPZ ponownie podkreślono, iż*Znaczenie pojęć użytych w niniejszym OPZ jest tożsame z definicjami przyjętymi we Wzorze Umowy ramowej (Załącznik nr 5 do SWZ) oraz Wzorze umowy wykonawczej (Załącznik nr 5A do SWZ).*

W świetle powyższego należy jednoznacznie stwierdzić, iż postanowienia pkt 1 ppkt 4 SOPZ oraz pkt 1 ppkt 16 SOPZ (uprzednio pkt 1 ppkt 18 SOPZ) odnoszą się do przedmiotowo odrębnych elementów przedmiotu zamówienia (odpowiednio ppkt 4 do Systemu SIEM, zaś ppkt 16 (wcześniej ppkt 18) do Oprogramowania dla Systemu SIEM). Tym samym należy stwierdzić, że w dokumentach zamówienia Zamawiający nie postawił wymogu, który jest kwestionowany przez Odwołującego2 w treści zarzutu obejmującego naruszenie art.art. 99 ust. 1 Pzp.

W związku z powyższym Izba oddaliła zarzut podniesiony w pkt 1 *petitum* odwołania.

Izba z analogicznych przyczyn oddaliła także drugi zarzut podniesiony w Odwołaniu2, ponieważ Odwołujący2 wskazując naruszenie w zakresie art. 106 ust. 2 Pzp odnosił treść kwestionowanego przedmiotowego środka dowodowego w odniesieniu do wymogu, który nie został postawiony przez Zamawiającego w dokumentach zamówienia. Zgodnie z treścią Rozdziału IX pkt 2 ppkt 2.1.1. Zamawiający w celu potwierdzenia, że oferowane dostawy spełniają określone przez Zamawiającego w opisie przedmiotu zamówienia wymagania, wymagał złożenia wraz z ofertą certyfikatu wydany nie wcześniej niż w 2020 roku przez akredytowane laboratorium Common Criteria potwierdzający, że oferowany System SIEM spełnia wymogi bezpieczeństwa Common Criteria for IT Security Evaluation. Z kolei wymóg dotyczący dostarczenia najnowszej wersji dotyczył zgodnie z pkt 1 ppkt 16 SOPZ (uprzednio pkt 1 ppkt 18 SOPZ) Oprogramowania dla Systemu SIEM i Systemu SOAR na dzień dostarczenia licencji
tj. etapu realizacji umów wykonawczych i zgodnie z definicją zawartą w § 1 ust. 1 pkt 10 Wzoru Umowy Ramowej odnosi się do Oprogramowania rozumianego jako całość programów komputerowych, aplikacji oraz wszelkiego pozostałego software'u, w tym oprogramowanie agentów instalowanych na stacjach końcowych oraz usługi zdalnego zarządzania oprogramowaniem agentów wchodzących w skład Systemu, bądź z nim związanych, umożliwiających realizację funkcjonalności Systemu zgodnie z Umową oraz OPZ.

Mając powyższe na względzie w ocenie Izby zarzut podniesiony w odwołaniu nie potwierdził się i Odwołanie2 w tym zakresie podlegało oddaleniu.

Zawarty w Odwołaniu2 zarzut naruszenia art. 99 ust. 4 Pzp odnoszący się do opisania przedmiotu zamówienia w sposób mogący utrudniać uczciwą konkurencję z uwagi na wymaganie, aby zaoferowany system SIEM był zakwalifikowany w opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów lub w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów, był uzasadniony.

Jak już wskazano uprzednio zamawiający ma prawo, jak i obowiązek opisać przedmiot zamówienia z uwzględnieniem swoich obiektywnych i uzasadnionych potrzeb. Takie potrzeby mogą powodować, że liczba wykonawców zdolnych do wykonania zamówienia będzie ograniczona. Fakt, że na rynku występują wykonawcy nieprodukujący danego przedmiotu zamówienia lub też dla których jego realizacja jest utrudniona czy wymaga pewnego dostosowania oferowanego przez nich produktu do wymagań zamawiającego, nie przesądza jeszcze o naruszeniu zasady uczciwej konkurencji. Dla stwierdzenia takiego naruszenia niezbędne jest zbadanie i ocena co najmniej kilku okoliczności związanych z danym zamówieniem, w szczególności takich jak kształt rynku, którego zamówienie dotyczy oraz skutki ograniczenia konkurencji dla ilości potencjalnych wykonawców mogących ubiegać się o uzyskanie zamówienia i z drugiej strony waga potrzeb zamawiającego, których realizacji takie ograniczenie służy. Opis przedmiotu zamówienia musi uwzględniać potrzeby konkretnego zamawiającego i jeżeli potrzeby te są zasadne, przedmiot zamówienia może być opisany w sposób ograniczający konkurencję. Zatem dopuszczalność poziomu ograniczenia konkurencyjności jest warunkowana uzasadnionymi potrzebami zamawiającego w tym zakresie.

W przedmiotowym postępowaniu niesporne jest, iż wprowadzony w pkt 1 ppkt 1 SOPZ wymóg o treści:

*1.System SIEM musi być dojrzałym, uznanym na rynku produktem – jako potwierdzenie spełnienia wymagania uznane będzie:*

*1.1.zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Gartner, dotyczącym rozwiązań klasy SIEM w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert)*

*lub*

*1.2. zakwalifikowanie oferowanego Systemu SIEM w niezależnym opracowaniu firmy badawczej Forrester Research, Inc. dotyczącym rozwiązań klasy Security Analytics Platforms w obszarze liderów (w raportach najbardziej aktualnych na dzień składania ofert).*

ogranicza konkurencję w przedmiotowym postępowaniu, gdyż zawęża grono potencjalnych rozwiązań do produktów sześciu producentów. W związku z tym na Zamawiającym ciążył obowiązek wykazania, że określenie tak sformułowanego wymogu jest uzasadnione jego konkretnymi, w pełni uzasadnionymi potrzebami. Tymczasem stanowisko zaprezentowane w odpowiedzi na odwołanie, jak również w toku rozprawy wskazuje, że Zamawiający nie sprostał temu wymogowi.

W prezentowanym stanowisku Zamawiający szeroko podkreślał rangę, renomę i uznanie na rynku raportów Gartner oraz Forrester. Wskazywał, że raporty te służą do podejmowania strategicznych decyzji, są powszechnie cenione, posiadają pewną metodologię oraz niezależność oraz powstają z ukierunkowaniem na konkretne obszary. Argumenty te w żaden sposób nie referowały jednak do uzasadnionych potrzeb Zamawiającego związanych z nabywanym przedmiotem zamówienia, lecz stanowiły subiektywną ocenę komercyjnych rozwiązań funkcjonujących na rynku raportów firm badawczych oceniających dostępne na rynku technologii cechującą się znacznym stopniem uznaniowości. Za takie należy uznać podnoszone argumenty odnoszące się do powszechnego uznania tych raportów, ich niezależności, obiektywizmu czy ukierunkowania na konkretne obszary. Brak jest podstaw – a przynajmniej Zamawiający takich okoliczności nie przywołał – dla stwierdzenia, że wyłącznie wskazanym w SOPZ raportom można przypisać takie cechy.

Za zasadnością wprowadzenia do opisu przedmiotu zamówienia kwestionowanego wymogu nie może przemawiać fakt posługiwania się raportami firmy Gartner i Forrester przez innych zamawiających w opracowanej przez nich dokumentacji postępowania. Należy ponownie podkreślić, że w przypadku wprowadzenia zapisów ograniczających konkurencję czy krąg potencjalnych wykonawców, musi to wynikać z konieczności wynikającej z konkretnych cech czy właściwości przedmiotu danego zamówienia, popartych w pełni uzasadnionymi potrzebami Zamawiającego. Tym samym przywoływana argumentacja odwołuje się nie do takich potrzeb czy wymagań, lecz do okoliczności zewnętrznych, niezwiązanych z przedmiotem zamówienia.

Podobnie należy w tym kontekście ocenić argumentację Zamawiającego odwołującą się do orzecznictwa Krajowej Izby Odwoławczej jako nieodwołującą się do przedmiotu zamówienia. Ponownie w kontekście tego argumentu należy wskazać, iż nie jest kwestionowana wartość merytoryczna poszczególnych raportów, lecz powiązanie tejże treści merytorycznej z elementami przedmiotu zamówienia, czego Zamawiający nie wskazał. Niezależnie od powyższego należy zaznaczyć, że przywołane orzeczenia dotyczyły odmiennych stanów faktycznych (tj. zastosowania raportu Gartnera jako elementu kryterium oceny ofert bądź kryterium równoważności), zaś w orzeczeniach dotyczących

zamieszczenia tego raportu jako elementu opisu przedmiotu zamówienia odmienne były podstawy zarzutów w ramach których kwestionowane było zastosowanie takich raportów.
W odniesieniu do przywoływanej przez Zamawiającego argumentacji związanej z ukierunkowaniem działalności firm Gartner oraz Forrester na podmioty sektora publicznego, ponownie próżno w tych argumentach doszukiwać się odwołania do kwestii związanych z przedmiotem zamówienia jakim jest dostawa określonych rozwiązań informatycznych. Zamawiający w żaden sposób nie wskazał w jaki sposób profil działalności podmiotów sporządzających określone raporty przekłada się na konieczność wprowadzenia w SOPZ wymogu ograniczającego istotnie krąg potencjalnych wykonawców, na jakie konkretne rozwiązania technologiczne, funkcjonalne czy jakościowe przedmiotu zamówienia taki profil działalności wpływa.
W dalszej kolejności Zamawiający podnosił, że wskazanie w SOPZ raportów konkretnych dostawców - Gartner oraz Forrester i dopuszczający możliwość zaoferowania wyłącznie takich rozwiązań, które znajdują się w obszarze liderów w raportach tych firm, jest odzwierciedleniem wyboru Zamawiającego, który - kierując się obiektywnymi potrzebami i celem postępowania - opowiedział się za produktami/rozwiązaniami sprawdzonymi, które cechuje wysoka dojrzałość technologiczna, potwierdzona stosownym raportem bezstronnej i niezależnej organizacji. W tym kontekście Zamawiający wskazał, że rozwiązanie pozyskane w ramach przedmiotowego postępowania ma zapewnić bezpieczeństwo cyfrowe jednostek wymiaru sprawiedliwości i z uwagi na powyższe konieczne jest wprowadzenie wymagań zapewniających oprogramowanie skuteczne, bezpieczne, o wysokim stopniu niezawodności i zaawansowanym stopniu rozwoju. Celem postępowania jest bowiem jak wskazał Zamawiający zapewnienie maksymalnej ochrony bezpieczeństwa danych zgromadzonych w systemach informatycznych Sądów Powszechnych. W świetle tak sformułowanych uzasadnionych potrzeb i wymagań oraz celu postępowania Zamawiający wprowadził do SOPZ wymóg, który w jego ocenie ma gwarantować dojrzałość oferowanych w postępowaniu rozwiązań, weryfikowaną określonym odniesieniem do raportu Gartner (kwadrat liderów) lub Forrester. Odniesienie to pozwala bowiem uzyskać rozwiązania sprawdzone, funkcjonujące na rynku od dłuższego czasu, cieszące się dobrą opinią i uznaniem, oferowane przez producentów, mających ustabilizowaną pozycję rynkową, rozwijających
na szeroką skalę kanał sprzedaży, dystrybucji i wsparcia technicznego dla swoich produktów.
W ocenie Izby w świetle przedstawionych przez Zamawiającego okoliczności należy stwierdzić,
iż określenie sformułowanego przez Zamawiającego wymogu nie było zasadne w świetle jego konkretnych, uzasadnionych potrzeb.

Należy bowiem stwierdzić, iż wprowadzenie spornego wymogu Zamawiający uzasadnia koniecznością pozyskania rozwiązania o wysokiej dojrzałości technologicznej, zapewniającego skutecznie maksymalny poziom bezpieczeństwa ochrony danych zgromadzonych w systemach,
o wysokim stopniu niezawodności i zaawansowanym stopniu rozwoju. Konieczność ta wynika jak wskazuje Zamawiający z interesu publicznego jakim jest zapewnienia bezpieczeństwa cybernetycznego systemom informatycznym i infrastrukturze, przetwarzającym dane o wysokim stopniu poufności, w tym dane wrażliwe. Tak sformułowanych celów i potrzeb Zamawiającego Izba nie kwestionuje. Jednocześnie jednak Zamawiający w żaden sposób nie wykazał, w jaki sposób realizacja powyższych potrzeb zostanie zapewniona poprzez wprowadzenie kwestionowanego wymogu dopuszczającego możliwość zaoferowania wyłącznie takich rozwiązań, które znajdują się w obszarze liderów w raportach Gartner lub Forrester. Zamawiający nie wskazał w jaki sposób
z treści ww. raportów, stosowanych do ich sporządzenia metodologii czy też z których kryteriów podlegających ocenie w ramach raportu ma wynikać poziom bezpieczeństwa produktów, zaawansowanie technologiczne oprogramowania czy też inne parametry techniczne, jakościowe i funkcjonalne, istotne z punktu widzenia podnoszonych, uzasadnionych potrzeb Zamawiającego związanych z przedmiotem postępowania i do nich referujące. Zamawiający jako uzasadnienie wprowadzenia wymogu przywołuje bowiem zawarte w raportach treści i kryteria, które nie mają charakteru technicznego czy jakościowego związanego z poszczególnymi produktami, lecz które odnoszą się do cech i właściwości poszczególnych podmiotów oferujących rozwiązania. Jako kryteria oceny produktów w ramach raportów przywoływana przez Zamawiającego jest m.in. pozycja rynkowa podmiotów, skala posiadanych przez nich kanałów sprzedaży, dystrybucji i wsparcia technicznego, kondycja finansowa, zdolności organizacyjne, posiadanie stosownych procesów, systemów i polityk. W ocenie Izby nie sposób uznać, że przywoływane przez Zamawiającego kryteria oceny o charakterze podmiotowym zawarte w raportach stanowiły uzasadnienie dla wprowadzenia wymogu dopuszczającego możliwość zaoferowania wyłącznie rozwiązań, które znajdują się w obszarze liderów w raportach Gartner lub Forrester, mając na uwadze iż dla Zamawiającego podstawą do wprowadzenie takiego wymogu są potrzeby przedmiotowe (funkcjonalne i jakościowe) oferowanych produktów. W konsekwencji przywoływane przez Zamawiającego kryteria oceny i treść raportów Gartnera i Forrestera nie potwierdzają czy i w jakim stopniu oferowane rozwiązania spełniają wymogi wynikające z uzasadnionych potrzeb wskazanych przez Zamawiającego.

Wobec powyższego w ocenie Izby wprowadzenie wymogu, uzależniającego możliwość zaoferowania danego systemu SIEM od uwzględnienia tego rozwiązania w konkretnym raporcie konkretnej firmy nie wynika z obiektywnych potrzeb Zamawiającego wyrażonych w dokumentach zamówienia. Tym samym potwierdził się podniesiony w pkt 3 lit. a) Odwołania2 zarzut naruszenia art. 99 ust. 4 Pzp i odwołanie podlegało uwzględnieniu w tym zakresie.

Zawarty w Odwołaniu2 zarzut naruszenia art. 99 ust. 4 Pzp odnoszący się do opisania przedmiotu zamówienia w sposób mogący utrudniać uczciwą konkurencję z uwagi na sposób sformułowania formularza ofertowego nie był uzasadniony.
W załączniku nr 1 do SWZ pn. Formularz ofertowy, Zamawiający na potrzeby kalkulacji zawarł tabelę

| **TABELA 1 Zakup licencji** | **Cena jednostkowa licencji netto w PLN*** | **VAT w %** | **Cena jednostkowa licencji brutto w PLN*** | **Ilość licencji*** | **Wartość brutto w PLN** | **Nazwa i producent oferowanego Systemu**** |
|---|---|---|---|---|---|---|
| a | b | c | d (b + b x c) | e | f (d x e ) | g |
| **System SIEM** wraz z Oprogramowaniem i usługami wsparcia technicznego i Gwarancją | ……./….. | ….% | ……./…. | ……. | | |
| **System SOAR** wraz z Oprogramowaniem i usługami wsparcia technicznego i Gwarancją | ……./….. | ….% | ……./…. | ……. | | |

| | | | |
|---|---|---|---|
| | **RAZEM** | | |

Wraz z adnotacją:
*Przy dokonywaniu wyceny, w Tabeli 1 należy:*
*- uwzględnić wymagania ujęte w OPZ, w tym w szczególności wymogi wydajnościowe opisane w Rozdz. 11 OPZ „Wymagania w zakresie wydajności i pojemności",*
**podać przyjęte do wyceny ceny jednostkowe licencji, jednostki miary oraz ilości*
***System SIEM i System SOAR muszą pochodzić od tego samego producenta*
W ocenie Odwołującego2 Zamawiający oczekując takiej prezentacji oferty utrudnia uczciwą konkurencję poprzez wyłączenie możliwości zaoferowania systemów, które pozwoliłyby Zamawiającemu uzyskać oczekiwane przez niego funkcjonalności w ramach jednej licencji, a tym samym nie dopuścił sytuacji, w której wykonawca mógłby dostarczyć rozwiązanie, w którym SOAR jest integralną częścią Systemu SIEM i nie jest oddzielenie wyceniany. Zdaniem Odwołującego2 takie rozwiązanie nie znajduje oparcia w obiektywnie uzasadnionych potrzebach Zamawiającego i w sztuczny sposób ogranicza możliwość zaoferowania rozwiązań, zaś to czy Zamawiający otrzyma narzędzie SOAR wbudowane w system SIEM, które będzie spełniało wszystkie wymagania określone przez Zamawiającego, czy też dwa odrębne systemy SIEM i SOAR, nie ma znaczenia z punktu widzenia realizacji potrzeb Zamawiającego.

Mając na uwadze powyżej wskazane twierdzenia, Izba stwierdza, że Odwołujący2 nie wykazał zasadności przedmiotowego zarzutu. Izba na wstępie wskazuje analogicznie jak w przypadku Odwołania1, że to treść odwołania oraz wskazane przez wykonawcę okoliczności faktyczne potwierdzające zasadność naruszenia określonych przepisów Pzp i stanowią podstawę do wydania rozstrzygnięcia przez Izbę. Postępowanie przed Izbą stanowi postępowanie kontradyktoryjne, czyli sporne, a z istoty tego postępowania wynika, że spór toczą Strony postępowania i to one mają obowiązek wykazywania dowodów, z których wywodzą określone skutki prawne. Powołując się na naruszenie art. 99 ust. 4 Pzp na odwołującego nałożone jest w pierwszej kolejności zobowiązanie do uprawdopodobnienia przez wykonawcę możliwości ograniczenia konkurencji przez dokonany przez zamawiającego opis przedmiotu zamówienia.

W ocenie Izby w analizowanym stanie faktycznym Odwołujący2 nie uprawdopodobnił, że przyjęty przez Zamawiającego sposób prezentacji oferty skutkuje możliwością ograniczenia konkurencji, jak również że sposób ten nie jest uzasadniony obiektywnymi potrzebami Zamawiającego. Odwołujący2 poprzestał na zawarciu w treści zarzutu dokonanej ogólnikowo własnej oceny potrzeb Zamawiającego. Stwierdzenia te nie zostały jednak poparte jakąkolwiek szerszą argumentacją, analizą dostępnych rozwiązań czy dowodami potwierdzającymi stawiane tezy.

Izba w tym zakresie uznała za w pełni spójne i wiarygodne stanowisko Zamawiającego zawarte w odpowiedzi na odwołanie oraz przedstawione w toku rozprawy. Zamawiający wyjaśnił, że model dostawy odrębnie oprogramowania SIEM i SOAR przyjęty przez Zamawiającego wynika z jego obiektywnych potrzeb uzasadnionych sposobem organizacji i delegowania zadań w zakresie zarządzania zdarzeniami cyberbezpieczeństwa w jego organizacji. Zamawiający podkreślił, że nie potrzebuje równej (takiej samej) ilości licencji SIEM i SOAR, ani nie potrzebuje oprogramowania SIEM integralnie połączonego z oprogramowania SOAR. Przeciwnie, na 12 lokalizacji wdrożenia oprogramowania SIEM (realizacji zadań SIEM), Zamawiający użytkuje ok. 2 licencje oprogramowania SOAR – co wynika z wyżej przedstawionej struktury organizacyjnej i zadań realizowanych przez określone elementy tej struktury. Ponadto Zamawiający odwołując się do zasad wynikających z przepisów o finansach publicznych podkreślił, że w swojej organizacji identyfikuje różne zapotrzebowanie ilościowe na funkcje oprogramowania SIEM i SOAR i dopasowuje do tego swój proces zakupowy, aby środki wydane na to oprogramowanie wydać racjonalnie i efektywnie. Zamawiający nie widział podstaw do wydatkowania środków publicznych na funkcjonalności, których w swojej strukturze nie potrzebuje, albo nie potrzebuje ich w określonej ilości. Skoro zatem Zamawiający nie potrzebuje oprogramowania SIEM i SOAR jednocześnie, ani nie potrzebuje takiej samej ilości licencji SIEM i SOAR, to nie może ich w jego ocenie nabywać łącznie i łącznie za nie płacić.

Powyższych twierdzeń Zamawiającego nie kwestionował również sam Odwołujący2, wskazując iż celem postawionego zarzutu jest dopuszczenie rozwiązań, które można opłacić jedną opłatą licencyjną, gdyż w jego ocenie architektura i uwarunkowania techniczne nie uzasadniają wyceny i rozliczenia odrębnie wyłącznie dla systemu SIEM i systemu SOAR. W tym miejscu Izba pragnie w szczególności zauważyć, że treść formularza nie uniemożliwia zaoferowania tego samego systemu (tj. rozwiązania, w którym System SOAR jest integralną częścią Systemu SIEM) odrębnie bądź to jako Systemu SIEM bądź Systemu SOAR. Mając na uwadze treść formularza, w szczególności fakt iż nie została przez Zamawiającego wskazana liczba licencji poszczególnych typów systemów, jak również podnoszoną przez Zamawiającego okoliczność że nie jest wymagana taka sama ilość licencji dla systemów SIEM i SOAR, jak również że nabycie jednego z tych systemów nie wiąże się automatycznie i nierozerwalnie z koniecznością nabycia drugiego rodzaju systemu, wycena rozwiązania w którym system SOAR jest narzędziem wbudowanym w system SIEM, nie musi się wiązać z zawyżeniem wyceny czy dublowaniem kosztu.

W zakresie przedmiotowego zarzutu Odwołanie2 należało zatem oddalić, o czym orzeczono w punkcie 4. wyroku.

O kosztach postępowania odwoławczego o sygn. akt KIO 3399/23 orzeczono stosownie do jego wyniku na podstawie art. 575 oraz art. 574 PrZamPubl, a także w oparciu o przepisy § 5 pkt 1 oraz § 8 ust. 2 zdanie pierwsze rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz.U. z 2020 r. poz. 2437 ze zm.) zaliczając na poczet kosztów niniejszego postępowania odwoławczego uiszczony przez Odwołującego1 wpis w wysokości 15.000 złotych oraz uzasadnione koszty poniesione przez Zamawiającego z tytułu wynagrodzenia pełnomocnika w wysokości 3.600 zł ustalone na podstawie spisu kosztów złożonego do akt sprawy (łącznie 18 600 zł).

O kosztach postępowania odwoławczego o sygn. akt KIO 3427/23 orzeczono stosownie do jego wyniku na podstawie art. 575 oraz art. 574 Pzp, a także w oparciu o przepisy § 5 pkt 1 oraz § 8 ust. 2 zdanie pierwsze rozporządzenia Prezesa Rady Ministrów z dnia 30 grudnia 2020 r. w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz.U. z 2020 r. poz. 2437 ze zm.) zaliczając na poczet kosztów niniejszego postępowania odwoławczego uiszczony przez Odwołującego1 wpis w wysokości 15.000 złotych oraz uzasadnione koszty poniesione przez Zamawiającego z tytułu wynagrodzenia pełnomocnika w wysokości 3.600 zł ustalone na podstawie spisu kosztów złożonego do akt sprawy (łącznie 18 600 zł).

Odwołanie2 okazało się zasadne w części 1/4 oraz chybione w części 3/4. Odpowiedzialność za wynik

postępowania ponosi zatem Odwołujący w części 3/4 i Zamawiający w części 1/4.

Odwołujący poniósł dotychczas koszty postępowania odwoławczego w wysokości 15 000 zł tytułem wpisu od odwołania oraz kosztów pełnomocnika, tymczasem odpowiadał za nie do wysokości 13 950 zł (18 600 zł x 3/4). Wobec powyższego Izba zasądziła od zamawiającego na rzecz odwołującego kwotę 1 050 zł (15 000 zł – 13 950 zł), stanowiącą różnicę pomiędzy kosztami postępowania odwoławczego poniesionymi przez Odwołującego2, a kosztami za jakie Odwołujący2 odpowiadał w świetle jego wyniku.

Mając na uwadze powyższe Izba orzekła jak w sentencji.

Przewodniczący:……...…

……...…

……...…