sygn. akt KIO 2423/23

POSTANOWIENIE
z dnia 30 sierpnia 2023 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodniczący:Monika Banaszkiewicz

Członkowie: Marek Bienias

Adriana Urbanik

Protokolant:Mikołaj Kraska

po rozpoznaniu na posiedzeniu niejawnym z udziałem stron w dniu 30 sierpnia 2023 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 14 sierpnia 2023 r. przez wykonawcę**SOFTINET sp. z o.o. z siedzibą w Warszawie** w postępowaniu prowadzonym przez **Sąd Apelacyjny w Krakowie reprezentowany przez pełnomocnika - Centrum Zakupów dla Sądownictwa Instytucję Gospodarki Budżetowej,**
przy udziale wykonawcy **STRYVE CEE sp. z o.o. z siedzibą w Warszawie** zgłaszającego przystąpienie do postępowania odwoławczego po stronie odwołującego

postanawia:

1.umorzyć postępowanie odwoławcze,
2.nakazać zwrot z rachunku bankowego Urzędu Zamówień Publicznych na rzecz wykonawcy**SOFTINET sp. z o.o. z siedzibą w Warszawie**, kwoty 13 500 zł (słownie: trzynaście tysięcy pięćset złotych zero groszy), tytułem zwrotu 90% uiszczonego wpisu.

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

Przewodniczący:……..……..

Członkowie: ……
……
Sygn. akt: KIO 2423/23

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

Zamawiający – Sąd Apelacyjny w Krakowie reprezentowany przez pełnomocnika - Centrum Zakupów dla Sądownictwa Instytucję Gospodarki Budżetowej prowadzi z odpowiednim zastosowaniem przepisów ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz.U. z 2023 r. poz. 1605, dalej: „ustawa Pzp") postępowanie o udzielenie zamówienia publicznego w trybie przetargu nieograniczonego pn. „Dostawa rozwiązania informatycznego obejmującego funkcjonalność rozszerzonego wykrywania i reakcji na zagrożenia w różnych warstwach zabezpieczeń, zapewniająca kompleksową ochronę środowiska informatycznego przed atakami oraz świadczenie innych usług towarzyszących" nr post.: WZP-421-5/2023. Ogłoszenie o zamówieniu zostało opublikowane w Dzienniku Urzędowym Unii Europejskiej numer 2023/S 149-471902 z dnia 4 sierpnia 2023 r.

Informację stanowiącą podstawę do wniesienia odwołania odwołujący powziął w dniu 4 sierpnia 2023 r. – dzień zamieszczenia ogłoszenia w Dzienniku Urzędowym Unii Europejskiej numer 2023/S 149-471902.

W dniu 14 sierpnia 2023 r. do Prezesa Krajowej Izby Odwoławczej wpłynęło odwołanie wykonawcySOFTINET sp. z o.o. z siedzibą w Warszawie wobec postanowień treści Specyfikacji Warunków Zamówienia (dalej: „SWZ"), sporządzonych przez zamawiającego w zakresie:

I wymagań technicznych dot. oferowanego rozwiązania – załącznik nr 2 do SWZ Opis Przedmiotu Zamówienia [ZARZUT#1]:

1) **pkt 2 ppkt 7 załącznika nr 2 do SWZ Opis Przedmiotu Zamówienia** (dalej jako: „**OPZ**") **w zakresie** sformułowania następujących wymogów **[ZARZUT#1.1]**:
„Cały System, wraz z gromadzonymi danymi analitycznymi musi być szyfrowany kluczami szyfrującymi wygenerowanymi i zarządzanymi przez Odbiorcę i w taki sposób, aby była możliwość w każdej chwili odwołania bądź zmiany użytych kluczy szyfrujących"
2) **pkt 2 ppkt 10 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.2]**:
„Wszystkie składniki Systemu MUSZĄ być konfigurowalne i zarządzane przez jeden spójny interfejs. Nie dopuszcza się, aby składniki Systemu posiadały

oddzielne pulpity/konsole do zarządzania konkretnymi funkcjami bezpieczeństwa, a dostęp do nich realizowany jest przez pojedyncze logowanie (Single Sign-On)".

3) **pkt 2 ppkt 14 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.3]**:
„System MUSI umożliwiać przypisywanie użytkowników do grup użytkowników".

4) **pkt 2 ppkt 25 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.4]**:
„System MUSI umożliwiać skonfigurowanie okna czasu, po którym użytkownik zostanie automatycznie wylogowany z Systemu oraz posiadać możliwość automatycznego zawieszania kont użytkowników, którzy nie logowali się dłużej niż określona liczba dni".

5) **pkt 2 ppkt 31 OPZ** i sformułowania następujących wymagań **[ZARZUT#1.5]**:
„System MUSI posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową".

6) **pkt 2 ppkt 32 lit a-c OPZ** i sformułowania następujących wymogów **[ZARZUT#1.6]**:
„System MUSI posiadać możliwość instalacji oprogramowania agenta co najmniej dla następujących Systemów operacyjnych i środowisk:
a) Windows 7, 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)
b) Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,
c) Linux
i. Red Hat Enterprise Linux 7, 8 i 9
ii. SUSE Linux Enterprise Server 11, 12 i 15".

7) **pkt 2 ppkt 33 lit a i b OPZ** i sformułowania następujących wymogów **[ZARZUT#1.7]**:
„System MUSI umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
a) W formacie msi dla Systemów Windows,
b) W formacie rpm, deb i sh dla Systemów Linux,".

8) **pkt 2 ppkt 34 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.8]**:
„Pakiet instalacyjny agenta dla Systemów Windows, macOS, Linux i klastrów Kubernetes MUSI posiadać możliwość:
a) Przypisanie do hosta nieusuwalnego znacznika (w procesie instalacji agenta) , który może być wykorzystany do tworzenia dynamicznych grup hostów i określenia zakresu dostępu jaki posiada rola użytkownika,
b) Wyłączenia opcji wykonywania skryptów,
c) Wyłączenia opcji pobierania plików,
d) Wyłączenia opcji dostępu do linii poleceń.".

9) **pkt 2 ppkt 38 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.9]**:
„System MUSI posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta MUSI umożliwiać określenie takich parametrów jak:
a) Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja,
b) Maksymalnej liczby równolegle aktualizowanych agentów,
c) Możliwość zdefiniowania zakresu: tylko aktualizacje naprawcze, tylko aktualizacje naprawcze w ramach wskazanej nowej wersji, najnowsza wersja, najnowsza przedostatnia wersja,
d) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowej wersji,
e) Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z Systemu,
f) Źródła aktualizacji agenta".

10) **pkt 2 ppkt 40 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.10]**:
„System MUSI umożliwiać różnicowanie konfiguracji agenta i modułów bezpieczeństwa poprzez przypisanie rożnych profili konfiguracyjnych do wybranych grup hostów lub pojedynczych hostów".

11) **pkt 2 ppkt 58 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.11]**:
„System dla każdego wprowadzonego pojedynczego i złożonego wskaźnika kompromitacji MUSI wygenerować alarm(-y):

a) jeśli znacznik został odszukany w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)
b) jeśli znacznik zostanie odszukany w nowych danych telemetrycznych".

12) **pkt 2 ppkt 61 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.12]**:
„System MUSI umożliwiać globalne blokowanie uruchamiania/ładowania plików binarnych z wykorzystaniem funkcji skrótu SHA256".

13) **pkt 2 ppkt 66 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.13]**:
„W ramach incydentu System MUSI umożliwiać grupowanie:
a) powiązanych z incydentem użytkowników,
b) Hostów,
c) Plików,
d) Domen,
e) Adresów IP".

14) **pkt 2 ppkt 69 OPZ** i sformułowania następujących wymogów **[ZARZUT#1.14]**:
„System MUSI umożliwiać zarządzanie incydentami co najmniej w następującym zakresie:
a) Przypisanie incydentu do analityka,
b) Zmianę stanu incydentu: badany, false positive, true positive, duplikat, testy,
c) Dodawanie notatek,
d) Komunikacja z innymi analitykami,
e) Raportowanie czasu MTTR."

15) **pkt 2 ppkt 72 lit. a, c, e, i-k, t ppkt i-ii, v oraz y OPZ** i sformułowania następujących wymogów **[ZARZUT#1.15]**:
„Agent dla Systemów operacyjnych z rodziny Windows:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
c) MUSI umożliwiać:
i. Ukrycie ikony agenta w zasobniku Systemowym,
ii. Wyłączenie powiadomień o zablokowanych zagrożeniach,
iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej,
iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego,
v. Użycie komunikatów i powiadomień w języku Polskim,
vi. Zarządzanie host firewallem hosta z wykorzystaniem Windows Filtering Platform,
vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu,
viii. Weryfikację stanu szyfrowania dysków,
ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, ktore zostały usunięte,
x. Usuwanie plików po SHA256 i po wskazaniu ścieżki do pliku,
(…)
e) powinien posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptow python.
(…)
i) MUSI posiadać możliwość blokowania uruchamiania programów z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.
j) MUSI posiadać możliwość blokowania uruchamiania programów ze wskazanych lokalizacji w Systemie plików.
k) MUSI posiadać możliwość blokowania uruchamiania programów z zasobów sieciowych poza wybranymi ścieżkami.
(…)
t) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami

binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host oraz poza terytorium Unii Europejskiej),
(…)
v) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host oraz poza terytorium Unii Europejskiej),
iii. Lokalna analiza statyczna.
(…)
y) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie".

16) **pkt 2 ppkt 73 lit. a, c, e, k ppkt i-ii, n OPZ** i sformułowania następujących wymogów **[ZARZUT#1.16]**:

„Agent dla Systemów operacyjnych z rodziny macOS:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
c) MUSI umożliwiać:
i. Ukrycie ikony agenta w zasobniku Systemowym,
ii. Wyłączenie powiadomień o zablokowanych zagrożeniach,
iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej,
iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego,
v. Użycie komunikatów i powiadomień w języku Polskim,
vi. Zarządzanie firewallem hosta,
vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu,
viii. Weryfikację stanu szyfrowania dysków,
ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte,
x. Usuwanie plików po SHA256 i po ścieżce.
(…)
e) powinien posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptów python.
(…)
k) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host oraz poza terytorium Unii Europejskiej),
(…)
n) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej

MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie".

17) **pkt 2 ppkt 74 lit. a, e, k ppkt i-ii, n OPZ** i sformułowania następujących wymogów **[ZARZUT#1.17]**:

„Agent dla Systemów operacyjnych z rodziny Linux i klastrów Kubernetes:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Z komponentu pośredniczącego,
iii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
e) MUSI posiadać wbudowany moduł obsługujący skrypty python w wersji 3.7 lub nowszy i możliwość uruchamiania wbudowanych i własnych skryptow python.
(…)
k) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host oraz poza;
(…)
n) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie".

18) **pkt 2 ppkt 76 lit. e i g OPZ** i sformułowania następujących wymogów **[ZARZUT#1.18]**:

„76. Agent dla Systemów operacyjnych iOS:
(…)
e) MUSI zapewniać ochronę przed podejrzanymi połączeniami głosowymi (ochrona przeciw vishingowa),
(…)
g) MUSI mieć opcję okresowego przypominania o konieczności restartu telefonu.".

W zakresie powyższych postanowień SWZ odwołujący zarzucił zamawiającemu naruszenie:

1) **art. 99 ust. 1 i ust. 4 w zw. z art. 16 pkt 1 i 3 PZP** poprzez opisanie przedmiotu zamówienia w sposób niejednoznaczny, niewyczerpujący i nieuwzględniający wszystkich okoliczności mających wpływ na sporządzenie oferty przez wykonawców oraz w sposób uniemożliwiający uczciwą konkurencję, naruszający zasadę równego traktowania wykonawców oraz nieproporcjonalny do przedmiotu zamówienia, poprzez sformułowanie powyższych wymagań, w sposób który wprost wskazuje na rozwiązanie oferowane przez jednego producenta – Palo Alto Networks, Inc. (dalej: „**Palo Alto Networks**") i rozwiązanie Palo Alto Cortex XDR– co w konsekwencji prowadzi do uniemożliwienia złożenia konkurencyjnej oferty przez wykonawców oferujących rozwiązania w pełni zgodne z wymaganiami i potrzebami Zamawiającego.

Stawiając powyższe zarzuty odwołujący wniósł o nakazanie zamawiającemu:

1) **modyfikacji wymagania z pkt 2 ppkt 7 OPZ** poprzez jego usunięcie z treści SWZ;

2) **modyfikacji wymagania z pkt 2 ppkt 10 OPZ** poprzez jego usunięcie z treści SWZ.

3) **modyfikacji wymagań z pkt 2 ppkt 14 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją lub jego usunięcie:

*„System MUSI umożliwiać **przypisywanie użytkowników do grup***

użytkowników zarządzanie uprawnieniami pojedynczych jak i wielu użytkowników*”.*

4) **modyfikacji wymagań z pkt 2 ppkt 25 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją lub jego usunięcie:

„System MUSI umożliwiać skonfigurowanie okna czasu, po którym użytkownik zostanie automatycznie wylogowany z Systemu oraz posiadać możliwość ***automatycznego zawieszania kont użytkowników zawieszania lub kasowania kont użytkowników****, którzy nie logowali się dłużej niż określona liczba dni”.*

5) **modyfikacji wymagań z pkt 2 ppkt 31 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją lub jego usunięcie:

„System MUSI ***posiadać możliwość określenia strefy czasowej wykorzystywanej do reprezentowania znaczników czasowych w interfejsie zarządzania oraz formatu tego znacznika co najmniej w takim zakresie, aby uwidaczniał on strefę czasową wykorzystywać lokalną strefę czasową do reprezentowania znaczników czasowych w interfejsie zarzadzania.***

6) **modyfikacji wymagań z pkt 2 ppkt 32 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją lub jego usunięcie:

„System MUSI posiadać możliwość instalacji oprogramowania agenta co najmniej dla następujących Systemów operacyjnych i środowisk:
a) Windows 7, 8, 10 i 11 (włącznie ze środowiskiem Persistent oraz Non-Persistent VDI)
b) Windows Server 2012 R2, 2016 standard i core, 2019 standard i core oraz 2022,
c) Linux
i. Red Hat Enterprise Linux 7, 8 i 9
ii. SUSE Linux Enterprise Server ***11****, 12 i 15*
iii. Ubuntu 18.04 LTS, 20.04 LTS i 22.04 LTS
iv. Oracle Linux 6 i 7
v. CentOS 6,7 i 8
vi. Debian 9, 10 i 11
d) macOS 11.x, 12.x i 13.x
e) środowisko klastrów Kubernetes
f) Android 10,11 i 12
g) iOS 15.x i 16.x”.

7) **modyfikacji wymagań z pkt 2 ppkt 33 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:

„System MUSI umożliwiać wygenerowanie i pobranie pakietu instalacyjnego:
a) W formacie msi dla Systemów Windows,
b) W formacie rpm i deb ***i sh*** *dla Systemów Linux,”.*

8) **modyfikacji wymagań z pkt 2 ppkt 34 OPZ** poprzez jego usunięcie z treści SWZ.

9) **modyfikacji wymagań z pkt 2 ppkt 38 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:

„System MUSI posiadać możliwość skonfigurowania manualnej i automatycznej aktualizacji agenta dla wskazanych grup hostów. Polityka automatycznej konfiguracji agenta MUSI umożliwiać określenie takich parametrów jak:
a) Dnia tygodnia i zakresu czasu, w którym wykonywana jest aktualizacja,
b) Maksymalnej liczby równolegle aktualizowanych agentów,
c) Możliwość zdefiniowania zakresu: tylko aktualizacje naprawcze, tylko aktualizacje naprawcze w ramach wskazanej nowej wersji, najnowsza wersja, najnowsza przedostatnia wersja,
d) Opóźnienie aktualizacji o wskazaną liczbę dni od publikacji nowej wersji,
e) Globalnego limitu na wykorzystanie pasma przy bezpośrednim pobieraniu z Systemu,
f) Źródła aktualizacji agenta”.

10) **modyfikacji wymagań z pkt 2 ppkt 40 OPZ** poprzez jego usunięcie z treści SWZ

11) **modyfikacji wymagań z pkt 2 ppkt 58 OPZ** poprzez zmianę treści wymagań

zgodnie z poniższą propozycją lub usunięcie pkt 2 ppkt 58 lit. a:
„System dla każdego wprowadzonego pojedynczego i złożonego wskaźnika kompromitacji MUSI ***wygenerować alarm(-y) pozwalać na****:*
a) sprawdzenie czy nie występował on w historycznych danych telemetrycznych (zgromadzonych przed dodaniem wskaźnika)
b) wygenerowanie alarmu jeśli znacznik zostanie odszukany w nowych danych telemetrycznych."
12) **modyfikacji wymagań z pkt 2 ppkt 61 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„System MUSI umożliwiać globalne blokowanie uruchamiania/ładowania plikow binarnych z wykorzystaniem funkcji skrótu ***MD5 lub SHA1 lub*** *SHA256".*
13) **modyfikacji wymagań z pkt 2 ppkt 66 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
*„****W ramach incydentu System MUSI umożliwiać grupowanie System MUSI umożliwiać, dla konkretnego incydentu, wyświetlenie listy****:*
a) powiązanych z incydentem użytkowników,
b) Hostów,
c) Plików,
d) Domen,
e) Adresów IP".
14) **modyfikacji wymagań z pkt 2 ppkt 69 OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„System MUSI umożliwiać, dla konkretnego incydentu, wyświetlenie listy W ramach incydentu System MUSI umożliwiać grupowanie:
a) powiązanych z incydentem użytkowników,
b) Hostów,
c) Plików,
d) Domen,
e) Adresów IP".
15) **modyfikacji wymagań z pkt 2 ppkt 72 lit. a, c, e, i-k, t ppkt i-ii, v oraz y OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„Agent dla Systemów operacyjnych z rodziny Windows:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
c) MUSI umożliwiać:
i. Ukrycie ikony agenta w zasobniku Systemowym,
ii. Wyłączenie powiadomień o zablokowanych zagrożeniach,
iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej,
iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego,
v. Użycie komunikatów i powiadomień w języku Polskim ***lub angielskim****,*
vi. Zarządzanie host firewallem hosta z wykorzystaniem Windows Filtering Platform,
vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu,
viii. Weryfikację stanu szyfrowania dysków,
ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte,
x. Usuwanie plików po SHA256 i po wskazaniu ścieżki do pliku,
(…)
e) powinien posiadać wbudowany moduł obsługujący ***języki skryptowe skrypty python w wersji 3.7 lub nowszy*** *i możliwość uruchamiania wbudowanych i własnych skryptów* ***python****.*

(…)
*i) MUSI posiadać możliwość **zatrzymania programów uruchomionych blokowania uruchamiania programów** z zewnętrznej pamięci masowej podłączonej na porcie USB i z napędów optycznych.*
*j) MUSI posiadać możliwość **zatrzymania programów uruchomionych blokowania uruchamiania programów** ze wskazanych lokalizacji w Systemie plików.*
*k) MUSI posiadać możliwość **zatrzymania programów uruchomionych blokowania uruchamiania programów** z zasobów sieciowych poza wybranymi ścieżkami.*
(…)
t) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi umożliwiając skonfigurowanie co najmniej następujących mechanizmów:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
*ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox **bezpośrednio na chronionym host oraz** poza terytorium Unii Europejskiej),*
(…)
*v) MUSI zapewnić ochronę **co najmniej dla plików Microsoft Word i Microsoft Excel zawierających znane i nieznane złośliwe makra przed znanymi i nieznanymi złośliwymi makrami co najmniej w plikach Microsoft Word i Microsoft Excel umożliwiając skonfigurowanie co najmniej następujących mechanizmów:***
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
*ii. Analiza dynamiczna w sandboxie producenta Systemu **(nie dopuszcza się uruchomienia funkcji sandbox bezpośrednio na chronionym host oraz poza terytorium Unii Europejskiej),***
iii. Lokalna analiza statyczna.
(…)
*y) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. **Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie**".*
16) **modyfikacji pkt 2 ppkt 73 lit. a, c, e, k ppkt i-ii, n OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„Agent dla Systemów operacyjnych z rodziny macOS:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
c) MUSI umożliwiać:
i. Ukrycie ikony agenta w zasobniku Systemowym,
ii. Wyłączenie powiadomień o zablokowanych zagrożeniach,
iii. Wyłączenie powiadomień o załączeniu i wyłączeniu izolacji sieciowej,
iv. Wyłączenie powiadomień o nawiązaniu zdalnego połączenia konsolowego,
*v. Użycie komunikatów i powiadomień w języku Polskim **lub angielskim**,*
vi. Zarządzanie firewallem hosta,
vii. Kontrolę urządzeń pamięci masowej na porcie USB w zakresie dopuszczenia dostępu do pamięci, dostępu w trybie tylko do odczytu i pełnego dostępu,
viii. Weryfikację stanu szyfrowania dysków,
ix. Wyszukiwanie plików po skrócie SHA256 i po ścieżce włączając w to pliki, które zostały usunięte,

x. Usuwanie plików po SHA256 i po ścieżce.
(…)
*e) powinien posiadać wbudowany moduł obsługujący **języki skryptowe skrypty python w wersji 3.7 lub nowszy i** możliwość uruchamiania wbudowanych i własnych skryptów **python**.*
(…)
k) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
*ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox **bezpośrednio na chronionym host oraz** poza terytorium Unii Europejskiej),*
(…)
*n) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. **Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie**".*
17) **modyfikacji pkt 2 ppkt 74 lit. a, e, k ppkt i-ii, n OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„Agent dla Systemów operacyjnych z rodziny Linux i klastrów Kubernetes:
a) MUSI posiadać możliwość pobierania aktualizacji agenta i aktualizacji modułów bezpieczeństwa:
i. Bezpośrednio z Systemu,
ii. Z komponentu pośredniczącego,
iii. Od innych hostów w tej samej podsieci (peer-to-peer).
(…)
*e) MUSI posiadać wbudowany moduł obsługujący **języki skryptowe skrypty python w wersji 3.7 lub nowszy** i możliwość uruchamiania wbudowanych i własnych skryptów **python**.*
(…)
k) MUSI zapewnić ochronę przed znanymi i nieznanymi złośliwymi plikami binarnymi wykorzystując co najmniej następujące mechanizmy:
i. Weryfikacja sha256 w bazie threat intelligence producenta Systemu,
*ii. Analiza dynamiczna w sandboxie producenta Systemu (nie dopuszcza się uruchomienia funkcji sandbox **bezpośrednio na chronionym host oraz** poza terytorium Unii Europejskiej);*
(…)
*n) MUSI posiadać możliwość manualnego wyłączenia izolacji sieciowej w przypadku, gdy agent utracił łączność z Systemem. Wyłączenie izolacji sieciowej MUSI być zabezpieczone hasłem. Każdy host MUSI posiadać własne hasło, tak aby można było je podać bezpiecznie użytkownikowi bez obawy, że inni użytkownicy zaczną wyłączać agenta. **Hasło MUSI być automatycznie rotowane przez System nie rzadziej niż co dwa tygodnie**".*
18) **modyfikacji pkt 2 ppkt 76 lit. e i g OPZ** poprzez zmianę treści wymagań zgodnie z poniższą propozycją:
„76. Agent dla Systemów operacyjnych iOS:
(…)
e) MUSI zapewniać ochronę przed podejrzanymi połączeniami głosowymi (ochrona przeciw vishingowa),
(…)
*g) **MUSI mieć opcję okresowego przypominania o konieczności restartu telefonu**".*

II. Kryteriów oceny ofert [Zarzut #2]

1) **Rozdział XIII pkt 2 lit b SWZ oraz pkt II.2.5) Ogłoszenia o zamówieniu [Zarzut #2.1] „Funkcjonalność F1 oferowanego Systemu" (F1)** – w zakresie jakim Zamawiający przyzna dodatkowe 20 pkt *„na podstawie oświadczenia Wykonawcy w Formularzu ofertowym oraz złożonego wraz z ofertą przedmiotowego środka dowodowego, wskazanego w Rozdz. IX pkt 2 ppkt 2.2.1. SWZ, w następujący sposób:*
- oferowany System zostanie uruchomiony w chmurze publicznej na terenie Polski (tj. chmura musi być hostowana w Polsce), a wszystkie elementy Systemu wykorzystywane przez Odbiorcę i Jednostki pozostaną w Polsce - 20 punktów
- oferowany System zostanie uruchomiony w chmurze publicznej na terenie Unii Europejskiej - 0 punktów".

2) **Rozdział XIII pkt 2 lit d SWZ oraz pkt II.2.5) Ogłoszenia o zamówieniu [Zarzut #2.2] „Funkcjonalność F3 oferowanego Systemu" (F3)** – w zakresie jakim Zamawiający przyzna dodatkowe 5 pkt *„na podstawie oświadczenia Wykonawcy w Formularzu ofertowym oraz złożonego wraz z ofertą przedmiotowego środka dowodowego, wskazanego w Rozdz. IX pkt 2 ppkt 2.2.1. SWZ, w następujący sposób:*
- oferowany System posiada opcję dystrybucji aktualizacji agenta w trybie peer-to-peer, celem zmniejszenia obciążenia łączy WAN i Internet - 5 punktów
- oferowany System nie posiada ww. funkcjonalności - 0 punktów".

18

3) **Rozdział XIII pkt 2 lit f SWZ oraz pkt II.2.5) Ogłoszenia o zamówieniu [Zarzut #2.3] „Funkcjonalność F5 oferowanego Systemu" (F5)** – w zakresie jakim Zamawiający przyzna dodatkowe 5 pkt *„na podstawie oświadczenia Wykonawcy w Formularzu ofertowym oraz złożonego wraz z ofertą przedmiotowego środka dowodowego, wskazanego w Rozdz. IX pkt 2 ppkt 2.2.1. SWZ, w następujący sposób:*
- oferowany System umożliwia uruchamianie skryptów python 3.x na MacOS, Linux oraz Windows na pojedynczej stacji roboczej lub ich grupach. Funkcjonalność musi być wbudowana w agenta i nie może wymagać dodatkowej instalacji środowiska uruchomieniowego python 3.x.- 5 punktów
- oferowany System nie posiada ww. funkcjonalności - 0 punktów".

W zakresie powyższego postanowienia SWZ odwołujący zarzucił zamawiającemu naruszenie następujących przepisów:

1) **art. 240 ust. 1 i 2 w zw. z art. 241 ust. 1 w zw. z art. 242 ust. 2 pkt 1-6 w zw. z art. 16 pkt 1-3 PZP** poprzez wprowadzenie niejednoznacznych, niezrozumiałych i dyskryminacyjnych kryteriów oceny ofert we wskazanym powyżej zakresie, które zostało sformułowane:

a) w sposób jednoznacznie faworyzujący rozwiązania określonego producenta (Palo Alto), który jest jedynym podmiotem spełniającym ww. kryteria,

b) w sposób uniemożliwiający uzyskanie punktacji w omawianym kryteriach przez producentów, którzy oferują równoważne usługi chmurowe zlokalizowane w Unii Europejskiej lub na terenie EWG (Europejskiej Wspólnoty Gospodarczej),

c) w sposób uniemożliwiający prawidłowe porównanie ofert.

2) **art. 16 pkt 1-3 PZP** poprzez prowadzenie Postępowania w sposób naruszający zasadę uczciwej konkurencji i równego traktowania wykonawców ze względu na opisanie kryteriów oceny ofert w sposób, który bezpodstawnie preferuje jednego producenta oprogramowania i uniemożliwia złożenie konkurencyjnych ofert wykonawcom, którzy oferują odpowiadające potrzebom Zamawiającego równoważne rozwiązania.

Stawiając powyższe zarzuty odwołujący wnosił o nakazanie Zamawiającemu:

1) dokonania modyfikacji SWZ poprzez usunięcie kryterium F1.

2) dokonania modyfikacji SWZ poprzez usunięcie kryterium F3.

3) dokonania modyfikacji SWZ poprzez usunięcie kryterium F5.

Odwołujący wnosił ponadto o:

1) zasądzenie od zamawiającego na rzecz odwołującego zwrotu kosztów postępowania odwoławczego, w tym zwrotu kosztów wynagrodzenia pełnomocnika, zgodnie z fakturą, która zostanie przedłożona na rozprawie,

2) dopuszczenie i przeprowadzenie dowodów na okoliczności wskazane w treści odwołania oraz dowodów, które

zostaną złożone przez Odwołującego na rozprawie.

Skład orzekający Krajowej Izby Odwoławczej, wyznaczony do rozpoznania niniejszej sprawy ustalił i zważył, co następuje:

Izba stwierdziła, że nie ma podstaw do odrzucenia odwołania, a także, że odwołujący posiada interes we wniesieniu odwołania.

Izba postanowiła dopuścić do udziału w postępowaniu odwoławczym wykonawcę STRYVE CEE sp. z o.o. z siedzibą w Warszawie, zgłaszającego przystąpienie do postępowania odwoławczego po stronie odwołującego.

W dniu 29 sierpnia 2023 r. (tj. przed dniem 30 sierpnia 2023 r., na który został wyznaczony termin posiedzenia) do akt sprawy wpłynęło pismo pełnomocnika Odwołującego, w którym oświadczył on, że cofa w całości odwołanie z dnia 14 sierpnia 2023 r. oraz wnosi o zwrot 90% wpisu od odwołania.

Mając powyższe na uwadze, Izba zważyła i ustaliła, co następuje:

Odwołujący złożył oświadczenie o cofnięciu odwołania, które zostało podpisane przez osobę umocowaną do podjęcia tej czynności, a jak stanowi art. 520 ustawy Pzp, odwołujący może cofnąć odwołanie do czasu zamknięcia rozprawy, a cofnięte odwołanie nie wywołuje skutków prawnych, jakie ustawa wiąże z wniesieniem odwołania do Prezesa Izby.

Biorąc pod uwagę powyższe, Izba uznała, że zachodzą podstawy do umorzenia postępowania odwoławczego w oparciu o art. 568 pkt 1 ustawy Pzp, w myśl którego Izba umarza postępowanie odwoławcze, w formie postanowienia, w przypadku cofnięcia odwołania.

Zgodnie z § 9 ust. 1 pkt 3 lit. a rozporządzenia w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania (Dz.U. z 2020 r. poz. 2437):

W przypadku umorzenia postępowania odwoławczego przez Izbę w całości na skutek cofnięcia odwołania przed otwarciem rozprawy najpóźniej w dniu poprzedzającym dzień, na który został wyznaczony termin rozprawy lub posiedzenia z udziałem stron lub uczestników postępowania odwoławczego - odwołującemu zwraca się 90% wpisu; w takim przypadku Izba orzeka o dokonaniu zwrotu odwołującemu z rachunku Urzędu kwoty uiszczonej tytułem wpisu, w wysokości stanowiącej 90% jego wartości.

Wobec powyższego orzeczono, jak w sentencji.

Przewodniczący: …….

Członkowie: …….

……