Sygn. akt KIO 614/26

WYROK

Warszawa, 23 marca 2026 r.

Krajowa Izba Odwoławcza:

Przewodnicząca: Agnieszka Trojanowska

Protokolantka: Wiktoria Ceyrowska

po rozpoznaniu na rozprawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej 9 lutego 2026 r. przez wykonawcę Trecom Wrocław Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, ul. Czyżewska 10 w postępowaniu prowadzonym przez zamawiającego Warszawski Uniwersytet Medyczny z siedzibą w Warszawie, ul. Żwirki i Wigury 61

Uczestnik po stronie zamawiającego:

wykonawca Clockwise Spółka z ograniczoną odpowiedzialnością Spółka Komandytowa z siedzibą w Warszawie, ul. Puławska 405A

orzeka:

1. Oddala odwołanie,

2. kosztami postępowania obciąża odwołującego i:

2.1. zalicza w poczet kosztów postępowania odwoławczego kwotę 15 000 zł 00 gr (piętnaście tysięcy złotych zero groszy) tytułem uiszczonego wpisu, 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem wydatków pełnomocnika odwołującego, 69 zł 00 gr (sześćdziesiąt dziewięć złotych zero groszy) tytułem kosztów dojazdu odwołującego, 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem wydatków pełnomocnika zamawiającego,

2.2. Zasądza od odwołującego na rzecz zamawiającego kwotę 3 600 zł 00 gr (trzy tysiące sześćset złotych zero groszy) tytułem zwrotu poniesionych przez zamawiającego wydatków pełnomocnika.

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

Przewodnicząca:…….

Sygn. akt KIO 614/25

Uzasadnienie

Postępowanie w trybie przetargu nieograniczonego pn. „Dostawa kompleksowych rozwiązań w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie Uczelni” nr postępowania: AEZ/S028/2025 w zakresie Pakietu nr 1 pn. Dostawa z uruchomieniem narzędzi do zarządzania bezpieczeństwem klasy XDR ogłoszono w Dzienniku Urzędowym Unii Europejskiej 7 listopada 2025 r., pod numerem 738468-2025.

30 stycznia 2026 r. zamawiający poinformował o wyborze oferty najkorzystniejszej.

9 lutego 2026 r. wykonawca Trecom Wrocław Spółka z ograniczoną odpowiedzialnością z siedzibą w Warszawie, ul. Czyżewska 10 wniósł odwołanie przez należycie umocowanego pełnomocnika. Do odwołania dołączono dowód jego opłacenia oraz przekazania zamawiającemu.

Odwołujący zarzucił zamawiającemu naruszenie:

1.art. 226 ust. 1 pkt 5 ustawy przez zaniechanie odrzucenia oferty niezgodnej z warunkami zamówienia, która to niezgodność polega na tym, że oferowany przez Clockwise system Cortex XDR produkcji Palo Alto Networks nie posiada funkcjonalności lub nie oferuje parametrów spełniających wymagania opisane przez zamawiającego w OPZ;

2.art. 239 ustawy w związku z art. 70 (1) §4 KC w związku art. 8 ust. 1 ustawy przez wybór oferty Clockwise, którą zgodnie z postanowieniem ust. 1 rozdz. XXII specyfikacji warunków zamówienia zamawiający winien był odrzucić jako ofertę, w stosunku do której zachodzą okoliczności, o których mowa w art. 226 ust. 1 ustawy;

Wniósł o nakazanie zamawiającemu:

1.unieważnienia czynności wyboru najkorzystniejszej oferty w zakresie Pakietu nr 1 upublicznionej w dniu 30.01.2026 r.;

2.odrzucenia oferty Clockwise w zakresie Pakietu nr 1 jako niezgodnej z warunkami zamówienia;

3.powtórzenia czynności badania i oceny ofert w postępowaniu w zakresie Pakietu nr 1;

3.4.zasądzenie od zamawiającego na rzecz odwołującego kosztów postępowania, w tym kosztów reprezentacji wg przedstawionych na rozprawie rachunków;

Odwołujący wskazał, że posiada interes we wniesieniu niniejszego odwołania w rozumieniu art. 505 ust. 1 ustawy.

Zamawiający w postępowaniu uzyskał 2 oferty w zakresie Pakietu nr 1 ofertę Clockwise na kwotę 495.562,92 zł oraz ofertą odwołującego opiewającą na kwotę 498.787,44 zł.
Oferta Clockwise jest niezgodna z warunkami zamówienia i powinna zostać odrzucona z postępowania, czego zaniechał zamawiający. W tej sytuacji odwołujący ma interes we wniesieniu odwołania i doprowadzania rozstrzygnięcia postępowania do stanu zgodnego z prawem, czyli odrzucenia oferty Clockwise.
Odrzucanie oferty Clockwise umożliwi wybór oferty odwołującego, a w konsekwencji uzyskanie przychodu i zysku z realizacji zamówienia. Zatem niewniesienie odwołania doprowadzi do szkody u odwołującego na skutek nieuzyskania przechodu i zysku z tego zamówienia
[zarzut naruszenia art. art. 226 ust. 1 pkt 5 ustawy - system Cortex XDR nie spełnia wymogu opasanego ust. 8 OPZ]
Zgodnie z postanowieniem ust. 8 załącznika nr 2.1. pt. Opis Przedmiotu Zamówienia Dostawa kompleksowych rozwiązań w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie Uczelni dla Pakietu 1 pn. Dostawa z uruchomieniem narzędzi do zarządzania bezpieczeństwem klasy XDR (dalej „OPZ") Zamawiający wymagał, aby oferowany System musi przechowywać przez 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena. Odwołujący wskazał, że oferowany przez Clockwise system Cortex XDR nie oferuje takiej możliwości.
W toku postępowania zamawiający wystąpił do Clockwise o wyjaśnienie treści tej oferty w tym zakresie. Clockwise w ramach wyjaśnień wskazał, że wymagania postanowieniem ust. 8 funkcja jest realizowane w sposób równoważny, zgodny z dokumentacją producenta. Clockwise wyjaśnia, że dostęp do wyników wyszukiwania możliwy jest nie przez API, a w modelu pobrania wyników i przeszukiwania ich lokalnie.
Zamawiający wu ust. 8 OPZ jasno określił, że wymaga, aby to System umożliwiał przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena. We własnych wyjaśnieniach Clockwise oświadczył, że przeszukiwanie nie jest realizowane za pomocą API. API służy tutaj tylko i wyłącznie do pobrania wszystkich danych, a przeszukiwanie jest realizowane w inny sposób. Zatem sam system Cortex XDR nie pozwala na przeszukiwanie danych przez API, a zaproponowane przez Clockwise przeszukiwanie realizowane jest już poza zaoferowanym systemem.
Zamawiający nie dopuścił, nie określił w zakresie tej funkcji kryteriów równoważności, ale jasny wymóg w OPZ, stąd Clockwise zaoferował rozwiązanie nie spełniające wymagań OPZ. Zatem zupełnie oczywiste jest niespełnienie wymagań postawionych przez zamawiającego w Opisie Przedmiotu Zamówienia przez oferowany przez Clockwise system Cortex XDR.
[system Cortex XDR nie spełnia wymogu opasanego ust. 10 pkt 10) 1 lit. b) OPZ]
Zgodnie z postanowieniem ust. 10 pkt 1) lit. b załącznika nr 2.1. pt. OPZ zamawiający wymagał, aby oferowany system posiadał możliwość instalacji agenta m.in. dla systemu operacyjnego Microsoft Windows 10 dla architektury procesorów x86-64 i arm64.
Zamawiający uznał to za wymóg nieodzowny, ponieważ brzmienie postanowienia ust. 10 OPZ wskazuje, że oferowany System musi posiadać możliwość instalacji agenta na co najmniej systemach operacyjnych wymienionych dalej w tym ustępie, w tym na systemie wskazanym w ust. 10 pkt 1) lit. b OPZ, tj. na Microsoft Windows 10 dla architektury procesorów x86-64 oraz arm64 właśnie.
Odwołujący wskazał, że ofertowany przez Clockwise system Cortex XDR nie ma możliwości instalacji agenta na systemie Windows 10 dedykowanym dla architektury procesora ARM64.
W toku postępowania zamawiający zwrócił się do Clockwise o wyjaśnienie tej kwestii wskazując, że zgodnie z dokumentacją Cortex XDR firmy Palo Alto ze strony https://docs-cortexpaloaltonetworks.com/r/Cortex-XDR-CompatibilityMatrix agent Cotrex XDR nie jest dostępny dla Windows 10 dla architektury ARM. Natomiast architektura ARM jest wspierana przez Cortex XDR tylko systemu operacyjnego Windows 11, co wynika z instrukcji ujawnionej na ww. stronie Palo Alto.
W ramach wyjaśnień Clockwise oświadczył, powołując się na aktualizację oprogramowania Cortex XDR Agent w wersji 9.0, że aktualne wsparcie dla systemów operacyjnych Windows opartych na procesorach RAM w oferowanym rozwiązaniu XDR jest dostępne.
Odwołujący wskazał, że przesłane przez Clockwise wyjaśnienie w żaden sposób nie wskazuje na to, że producent zapewnia wsparcie dla Windows 10 z architekturą ARM64. Uwidoczniona w dokumencie informacja wskazuje jedynie, że Cortex XDR jest dostępny dla bliżej nieokreślonego systemu Windows działającego na architekturze ARM 64.
Powyższe potwierdza fakt, że w styczniu 2026 roku producent Palo Alto wprowadził do oferty nową wersję Cortex XDR oraz nową wersję agenta numerowaną jako 9.1. Odnosząc się do tej najnowszej wersji systemu Cotrex XDR odwołujący podkreślił, że nawet w przypadku tej wersji oprogramowania producent nie wskazuje, aby był dostępny agent w wymaganej przez zamawiającego wersji dla Windows 10 dedykowanej dla architektury ARM64. Na stronie zawierającej

informacje producenta Palo Alto dla systemu Cotrex XDR producent wskazuje m.in.: że
To ensure maximum protection of your endpoints, Palo Alto Networks recommends that you always deploy the latest maintenance version for each agent release,
Czyli producent zaleca(tłumaczenie): Aby zagwarantować maksymalną ochronę punktów końcowych, firma Palo Alto Networks zaleca, aby zawsze wdrażać najnowszą wersję konserwacyjną dla każdej wersji agenta.
Dalej na tej stronie producent Palo Alto przedstawia tabele zawierające wskazanie systemów operacyjnych dla urządzeń końcowych, dla których Cortex XDR oferuje wsparcie.Producent wskazuje tamże: The following tables show the endpoint operating systems on which you can install each release of the Cortex XDR agent. These operating systems are also supported with supported Citrix and VMware virtual applications.Tłumaczenie: Poniższe tabele przedstawiają systemy operacyjne punktów końcowych, na których można zainstalować poszczególne wersje agenta Cortex XDR. Te systemy operacyjne są również obsługiwane przez aplikacje wirtualne Citrix i VMware.
Wg producenta Palo Alto Networks jego System Cortex XDR dla systemów Windows 10 i Windows 11 oferuje wsparcie dla następujących wersji, wg tabel: tu odwołujący wkleił tabele ze strony producenta dotyczące Windows 10 i Widows 11 oraz wskazania czy system i w jakich wersjach oferuje wsparcie.
Z tych tabel dla odwołującego jasno wynika, że zgodnie z oświadczeniem producenta Palo Alto jego system Cortex XDR nie dalej możliwości instalowania agenta dla architektury ARM64 dla Windows 10, ale daje możliwość instalowania agenta dla architektury ARM64 dla Windows 11. Wynika z tego, że Palo Alto nie uwzględnił architektury ARM64 dla Windows 10, ale uwzględnił architekturę ARM64 dla Windows 11 w ww. zestawieniach.
Jako że wspomniany dokument został opublikowany już w styczniu 2026, czyli po dacie złożenia ofert, absolutnie nie można przyjąć interpretacji, że zaoferowane przez Clockwise rozwiązanie Palo Alto Cortex XDR spełnia wymogi OPZ w zakresie wymogu określonego ust. 10 pkt 1) lit. b) OPZ.
[system Cortex XDR nie spełnia wymogu opasanego ust. 34 OPZ]
W ust. 34 OPZ zamawiający określił wymóg dotyczący izolacji skompromitowanego urządzenia końcowego (tzw. endpointa) precyzując, że: System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.
Odwołujący wskazał, że ofertowany przez Clockwise system Cortex XDR w trakcie trwania izolacji skompromitowanego endponita na serwerach Linux, poza połączeniami do systemu oraz protokołu DHCP, dopuszcza ruch DNS i HTTPS z siecią, co oczywiście wykracza poza dopuszczony warunkiem ruch do konsoli XDR.
W toku postępowania zamawiający wezwał Clockwise do wyjaśnień w tym zakresie i powołując się na treść dokumentacji producenta Palo Alto dla systemu Cotrex XDR dostępnej na stronie https://docs-cirtex.palpaltoworks.com/r/Cortex-XDR-4.x-Documentation/Initiate-a-LiveTerminal-sessions, z którego wynika, że po izolacji punkt końcowy pozwala na: ruch wychodzący DHCP i HTTPS dla użytkownika root i ruch DNS, a co stoi w sprzeczności z wymogiem ust. 34 OPZ.
W ramach wyjaśnień treści oferty Clockwise oświadczył, że: Według naszej wiedzy, dobrych praktyk i naszego doświadczenia związanego z wdrażaniem rozwiązań Cortex XDR, wymóg „w trakcie izolacji cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany” jest spełniony, ponieważ rozwiązanie w trybie izolacji blokuje ruch sieciowy endpointa z wyjątkiem kanału komunikacji z systemem zarządzającym oraz DHCP.
W dokumentacji znajduje się zapis "When you isolate an endpoint, you halt all network access on the endpoint except for traffic to Cortex XDR."(tłum. „Izolując punkt końcowy, zatrzymujesz cały dostęp do sieci na tym punkcie, z wyjątkiem ruchu do Cortex XDR.”). Jednocześnie wskazujemy, że w praktyce technicznej „połączenie do systemu” wymaga utrzymania niezbędnych zależności tego kanału DNS i HTTPS są warstwami technicznymi niezbędnymi do utrzymania połączenia z systemem zarządzającym. Wymóg OPZ dopuszcza ruch „do systemu”, a więc obejmuje również mechanizmy potrzebne do jego zestawienia i utrzymania takie jak DNS/FQDN oraz HTTPS/TLS.
Odwołujący wskazał, że wyżej przytoczone twierdzenie Clockwise o tym, jakoby wskazywane w instrukcji połączenia wychodzące izolowanego urządzenia końcowego przy użyciu kanałów DNS i HTTPS stanowi połączenie z systemem zarządzającym za pośrednictwem DNS i HTTPS jako warstwami technicznymi niezbędnymi do utrzymania połączenia z systemem zarządzającym, jest sprzeczne z ww. jasnym opisem technicznym zawartym w dokumentacji technicznej producenta Cortex XDR.
Clockwise opiera w tym zakresie swoje twierdzenie, wprost sprzeczne z oświadczeniami producenta Cortex XDR, o swoje przekonanie wynikające jakoby z wiedzy, dobrych praktyk i naszego doświadczenia związanego z wdrażanie rozwiązań Cortex XDR Clockwise. Natomiast opis przedmiotu zamówienia na dostawę oprogramowania bazuje na porównaniu dostępnych funkcjonalności oprogramowania, a nie dobrych praktykach wykonawcy.
Nieprawdą jest, że połączenia DNS oraz HTTPS są niezbędne dla zestawienia połączenia do konsoli zarządzania Cortex XDR, jak twierdzi Clockwise w wyjaśnienia treści swojej oferty. Połączenie do DNS jest niezbędne tylko w celu wskazania agentowi adresu IP, z którym powinien się skomunikować celem nawiązania połączenia do konsoli

administracyjnej. Połączenie to odbywa się do lokalnego lub globalnego serwera DNS i nie jest połączeniem do samej konsoli administracyjnej. Zatem wyjaśnienia Wykonawcy są niewiarygodne.
Odwołujący wskazał, że po uzyskaniu adresu IP połączenie do DNS jest połączeniem niezwiązanym z komunikacją z konsolą administracyjną i stanowi potencjalnie niebezpieczny kanał, który może zostać wykorzystany do infiltracji/eksfiltracji danych z izolowanego komputera co uwidacznia, że może to stanowić realne zagrożenie bezpieczeństwa. Dodatkowo agent może uzyskać połączenie do konsoli przez wpisanie w konfiguracji adresu IP do połączenia z konsolą administracyjną – wówczas sam agent nie potrzebuje połączenia z DNS dla realizacji połączenia z konsolą, a mimo to utrzymuje otwarte połączenie DNS. Stanowi to wprost brak spełnienia wymagania postawionego przez zamawiającego w ust. 34 OPZ.
Dodatkowo połączenie HTTPS jest połączeniem używanym powszechnie przy dostępie do stron internetowych – tym samym dopuszczenie tego ruchu powoduje, że zainfekowany komputer może łączyć się z dowolnymi zasobami w Internecie. Nie można zatem przyjąć interpretacji Clockwise, że jest to połączenie niezbędne by zrealizować łączność z konsolą administracyjna systemy Cortex XDR.
Podkreślił, że w ww. dokumentacji systemu Cortex XDR producent Palo Alto Networks zawarł się konkretny opis dotyczący izolacji:
Tu odwołujący wkleił fragment dokumentacji systemu w języku angielskim.
Co w przekładzie oznacza:
„Wyizolowanie punktu końcowego
Gdy izolujesz punkt końcowy, dochodzi do zablokowania dostępu do sieci z tego urządzenia końcowego z wyjątkiem ruchu do Cortex XDR. Służy to temu, aby skompromitowane urządzenie końcowe nie miało możliwości komunikacji z innymi punktami końcowymi, ograniczając mobilność atakującego w Twojej sieci. Po otrzymaniu przez agenta instrukcji by izolować urządzenie końcowe i wykonaniu tej akcji, Cortex XDR wskazuje status Izolowany. Aby zapewnić, że urządzenie końcowe pozostanie w izolacji, w czasie jej trwania dla izolowanych urządzeń nie są dostępne aktualizacje oprogramowania agenta.
Po izolacji punkt końcowy nadal pozwala na:
•Ruch wychodzący DHCP i HTTPS dla użytkownika root
•Ruch DNS”
Co oznacza, że uzyskanie/wskazanie statusu „isolated” w Cortex XDR determinuje już komunikację z konsolą zarządzającą w zakresie niezbędnym do zrealizowania cechy izolacji. Pomimo to producent Palo Alto wskazuje, że w tym stanie agent ma nadal możliwość podłączenia się do innych usług tj. DNS i HTTPS. Stoi to w jawnej sprzeczności z tym co zamawiający określił w wymaganiach OPZ.
[system Cortex XDR nie spełnia wymogu opasanego ust. 65 OPZ]
W ust. 65 OPZ zamawiający postawił wymóg dotyczący funkcjonalności zamawianego systemu polegający na tym, że Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.
Rozwiązanie Cortex XDR firmy Palo Alto Networks zaoferowane przez Clockwise nie posiada zdolności do usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel i pod tym względem oferta Clockwise jest wprost niezgodna wymogiem określonym przez zamawiającego w ust. 65 OPZ.
Zgodnie z dokumentacją producenta Cortex XDR dostępną na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.xDocumentation/Set-up-malware-prevention-profiles agent Cortex XDR umożliwia wykrycie złośliwych makr w plikach WORD i EXCEL, a następnie jego działanie ogranicza się do blokowania wykonania złośliwych makr zagnieżdżonych w dokumentach Microsoft Office (WORD, EXCEK) na endpointach z systemem Windows, co jest opisane w sekcji dotyczącej funkcji Office Files with Macros Examination (tłumaczenie: Pliki Office z weryfikacją makr) w dokumentacji dotyczącej konfiguracji profili zapobiegania złośliwemu oprogramowaniu. Instrukcja systemu Cortex XDR w odniesieniu do makr w plikach Mocrosoft Office wskazuje:
Tu odwołujący wkleił fragment dokumentacji producenta w języku angielskim.
Tłumaczenie:
3. Skonfiguruj opcje plików pakietu Office z funkcją badania makr. Agent Cortex XDR może analizować i zapobiegać uruchamianiu złośliwych makr osadzonych w plikach pakietu Microsoft Office (Word, Excel) na punktach końcowych systemu Windows.
PrzedmiotOpcje
Tryb akcjiBlokowanie Raportowanie
WyłączanieGdy agent Cortex XDR wykryje próby uruchomienia złośliwego oprogramowania, wykonuje skonfigurowaną akcję
Jak jednoznacznie widać możliwa jest akcja zablokowania (ang. Block), akcja powiadomienia o wykryciu złośliwego makra, ale bez blokowania (Report) oraz opcja wyłączenia tej funkcji (ang. Disabled).

Jako uzupełnienie, rozwiązanie to pozwala na usuwanie lub umieszczanie w kwarantannie całych plików uznanych za złośliwe, co jest opisane w części poświęconej funkcji Search and Destroy w oficjalnej dokumentacji administratora:https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/CortexXDR-3.x-Documentation/Search-and-destroy-malicious-files
Z dokumentacji producenta systemu Cortex XDR wynika, że system nie dysponuje wymaganą przez zamawiającego funkcjonalnością usunięcia wyłącznie złośliwego kodu makra z dokumentu z pozostawieniem niezmienionej resztę zawartości pliku Word/Excel, tak jak zostało to opisane w ust. 65 OPZ.
Działania reakcyjne agenta systemu Cortex XDR są zatem ograniczone do blokowania wykonania makra oraz usuwania lub kwarantanny całego pliku, a nie „oczyszczania" dokumentu z złośliwych makr. Nie można zatem ustanowić równoważności pomiędzy dostępnymi akcjami w rozwiązaniu Cortex XDR a ustanowionym w tym zakresie jasnym wymogiem zamawiającego.
[system Cortex XDR nie spełnia wymogu opasanego ust. 70 OPZ]
W ust. 70 OPZ zamawiający określił wymóg automatycznego skanowania pamięci masowej po jej przyłączeniu wskazując: Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB.
Oferowany przez Clockwise system Cortex XDR produkcji Palo Alto Networks nie realizuje funkcji automatycznego, natychmiastowego skanowania pamięci masowej w momencie podłączenia nośnika do portu USB.
Funkcja takiego skanu „on connect" nie jest dostępna w produkcie jako natywna możliwość wyzwalania malware-scanu bezpośrednio po wykryciu urządzenia USB.
Cortex XDR umożliwia jedynie skanowanie przyłączonych nośników wymiennych (removable media drives) w ramach okresowego skanowania malware (Periodic Scan, który jest konfigurowany w profilu Malware Security Profile → Endpoint Scanning → Periodic Scan, przez włączenie opcji „Scan Removable Media Drives"). W tym trybie nośniki USB są objęte cyklicznym skanem (np. tygodniowym lub miesięcznym), podczas gdy zamawiający jednoznacznie w wymaganiu wskazał, że nośnik USB musi być skanowany „natychmiast", co explicite wskazuje, że wymaga skanu uruchamianego automatycznie w chwili podłączenia urządzenia, a nie po określonym czasie.
System Cortex XDR oferuje funkcję Device Control, pozwalającą na kontrolowanie dostępu do urządzeń USB (m.in. blokowanie odczytu/zapisu, ograniczanie typów urządzeń oraz generowanie alertów i logów zdarzeń związanych z podłączaniem nośników) jednak funkcja ta służy do ograniczania ryzyka związanego z nośnikami wymiennymi, ale nie obejmuje automatycznego wyzwalania skanu wirusowego w momencie ich podłączenia.
[art. 239 ustawy w związku z art. 70 (1) §4 KC w związku art. 8 ust. 1 ustawy]
W postanowieniu ust. 1 rozdz. XXII SWZ zamawiający wskazał: Zamawiający odrzuci ofertę, w przypadku zaistnienia okoliczności, o których mowa w art. 226 ust. 1 ustawy.
Z uwagi na wyżej wykazane niezgodności treści oferty Clockwise z warunkami zamówienia, zamawiający winien był odrzucić ofertę tego wykonawcy na podstawie art. 226 ust. 1 pkt 5) ustawy.
Zgodnie z art. 70 (1) §4 KC Organizator od chwili udostępnienia warunków, a oferent od chwili złożenia oferty zgodnie z ogłoszeniem aukcji albo przetargu są obowiązani postępować zgodnie z postanowieniami ogłoszenia, a także warunków aukcji albo przetargu. Zatem zamawiający jako organizator przetargu od chwili ogłoszenia dokumentów zamówienia obowiązany jest do treści własnych dokumentów zamówienia w zakresie, w jakim związał się nimi.
Zatem zaniechanie odrzucenia oferty niezgodnej z warunkami zamówienia w świetle ust. 1 rozdz. XXII SWZ i dopuszczenie do wyboru w przetargu – postępowaniu takiej oferty stanowi naruszenie art. 70 (1) §4 KC w związku z art. 239 ustawy w taki zakresie, w jakim wadliwa oferta w ogóle brana jest pod uwagę przy wyborze najkorzystniejsze oferty i oceniania w ramach kryteriów oceny ofert wraz z innymi, niewadliwymi ofertami.
[konkluzja]
Zamawiający korzystając z uprawnienia określonego w art. 246 ust.2 ustawy ustalił cenę jedynym kryterium oceny ofert wskazując w uzasadnieniu zawartym w ust. 4 rozdz. XII SWZ, że w Postępowaniu kryteria oceny ofert zrezygnował z OPZ określa szczegółowe wymagania techniczne i funkcjonalne, będące wyznacznikiem jakości właściwej dla określonego segmentu systemów, odnoszące się do głównych cech funkcjonalnych pozostających w ofercie spośród kręgu wykonawców oferujących tego typu rozwiązania. Zatem postanowienia OPZ zawierają główne wymagania jakościowe odnoszące się do zamawianego systemu i przedmiot oferty powinien bezwzględnie im odpowiadać.
Oferowany przez Clockwise system Cortex XDR nie oferuje przynajmniej 5 opisanych odwołaniem funkcjonalności wymaganych bezwzględnie OPZ, tj. system Cortex XDR nie zapewnia wsparcia dla systemu Windows 10 dedykowanego dla procesora o architekturze ARM64; w trakcie izolacji skompromitowanego urządzenia końcowego na systemach Linux, poza jedynie dopuszczonymi połączeniami do systemu oraz protokołu DHCP, dopuszcza ruch DNS i HTTPS z siecią; agent Cortex XDR nie dysponuje możliwością usuwania złośliwych makr z plików Word i Excell, a jego zdolność reakcji ogranicza się do blokowania, raportowania, ewentualnie usunięcia całego pliku Word/Excell; wreszcie

agent Cortex XDR nie oferuje funkcjonalności automatycznego skanowania pamięci masowej po jej podłączeniu.
W kontekście wymogów określonych dla zamawianego systemu XDR system Cortex XDR nie wypełnia przynajmniej 5 wymogów OPZ i oferta Clockwise powinna być odrzucona z uwag na jej niezgodność z warunkami zamówienia, czego zamawiający zaniechał.
10 lutego 2026 r. zamawiający poinformował o wniesieniu odwołania.
12 lutego 2026 r. wykonawca Clockwise Spółka z ograniczoną odpowiedzialnością Spółka Komandy ul. Puławska 405A, 02-801 Warszaw zgłosił swój udział w postępowaniu odwoławczym po stronie zamawiającego wnosząc o oddalenie odwołania. Przystępujący działał przez należycie umocowanego pełnomocnika. Do zgłoszenia dołączono dowody jego przekazania stronom. Przystępujący wskazał, że zgodnie z podjętą przez Zamawiającego decyzją, jego oferta została uznana za najkorzystniejszą w części zamówienia objętej pakietem nr 1. Uwzględniając zarzuty wniesionego odwołania oraz sformułowane w nim żądania (odrzucenie oferty Przystępującego) jego uwzględnienie spowodowałoby pozbawienie przystępującego możliwości uzyskania zamówienia. W konsekwencji stwierdził, że posiada interes w rozstrzygnięciu wniesionego odwołania na korzyść zamawiającego tj. przez utrzymanie w mocy zaskarżonej przez odwołującego decyzji o wyborze oferty przystępującego jako najkorzystniejszej.
19 marca 2026 r. zamawiający złożył odpowiedź na odwołanie wnosząc o oddalenie odwołania w całości jako bezzasadnego.
Zamawiający nie zgodził się z zarzutami przedstawionymi w odwołaniu, jednocześnie odnosząc się merytorycznie do przedmiotowych zarzutów.
Zarzut nr 1: Ust. 8 OPZ – Przeszukiwanie IOC via API (180 dni) Wymóg: "System musi przechowywać przez 180 dni umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe (domena). Zarzut: Cortex XDR nie umożliwia przeszukiwania IOC poprzez API. API służy tylko do pobrania wszystkich danych, a przeszukiwanie realizowane jest lokalnie poza systemem. Zamawiający wymagał, aby SAM SYSTEM przeszukiwał via API, czego Cortex XDR nie oferuje.
Wyjaśnienie Clockwise (z 14.01.2026): Funkcja realizowana w sposób równoważny zgodnie z dokumentacją producenta. Dostęp do wyników wyszukiwania możliwy przez model pobrania wyników i przeszukiwania ich lokalnie.
Ocena: 1.OPZ nie definiuje architektury technicznej – wymóg "via API" oznacza możliwość programowego dostępu do funkcji przeszukiwania, niekonkretną implementację query processing
2. Równoważność funkcjonalna – Cortex XDR Platform API oferuje endpoint /public_api/v1/indicators/get z parametrami filtrowania:
- field: indicator, type (hash/ip/domain_name)
- operator: EQ, IN, GTE, LTE
- search_from/to: paginacja wyników
- Zwraca obiekty IOC z atrybutami zgodnie z wymogami OPZ
3. Standard rynkowy REST API – model "pobierz z filtrami + przetwarzaj lokalnie" stosowany powszechnie (Elasticsearch, Splunk, Microsoft Defender).
Zamawiający dodatkowo wskazał, że Krajowa Izba Odwoławcza w swoim orzecznictwie – wielokrotnie uznawała, że OPZ nie może narzucać konkretnych rozwiązań technicznych, jeśli cel zostaje osiągnięty, co potwierdza orzeczenie KIO 1234/19 oraz KIO 2456/20.
Zarzut nr 2: Ust. 10 pkt 1 lit. b OPZ – Windows 10 ARM64 Wymóg: "Oferowany System musi posiadać możliwość instalacji agenta na co najmniej systemach operacyjnych: [...] Microsoft Windows 10 dla architektury procesorów x86-64 i arm64" Zarzut Trecom: Cortex XDR nie ma agenta dla Windows 10 ARM64. Dokumentacja producenta (Cortex XDR Compatibility Matrix, styczeń 2026, wersja 9.1) wyraźnie rozróżnia: - Windows 10: x86-64 (wsparte) - Windows 11: x86-64, ARM64 (wsparte) Brak Windows 10 ARM64 w tabelach zgodności. Clockwise powołał się na wersję 9.0, ale nawet najnowsza wersja 9.1 nie potwierdza wsparcia dla W10 ARM64. Wyjaśnienie: Aktualizacja oprogramowania Cortex XDR Agent w wersji 9.0+ zapewnia wsparcie dla systemów operacyjnych Windows opartych na procesorach ARM, w tym Windows 10.
Ocena:
1. Deklaracja producenta vs. dokumentacja – jeśli Palo Alto Networks oficjalnie potwierdzi wsparcie W10 ARM64 (np. przez Technical Support ticket), dokumentacja publiczna może być nieaktualna.
2. Zalecenie producenta – "Always deploy the latest maintenance version" sugeruje ciągłe rozszerzanie wsparcia.
3. Faktyczne potrzeby zamawiającego – WUM nie posiada urządzeń z Windows 10 ARM64 (inwentaryzacja IT: 0 sztuk), wymóg może być teoretyczny
4. Zasada proporcjonalności – odrzucenie oferty za brak wsparcia dla nieistniejącej w infrastrukturze architektury byłoby nieproporcjonalne.
5. Jednoznaczność tabeli zgodności – Palo Alto wyraźnie rozróżnia W10 i W11 w kontekście ARM64.

Zarzut nr 3: Ust. 34 OPZ – Izolacja sieciowa endpoint Wymóg OPZ: "System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany."
Zarzut: Cortex XDR w trakcie izolacji endpointów na serwerach Linux dopuszcza:
- Ruch wychodzący DHCP (zgodnie z wymogiem)
- Ruch wychodzący HTTPS dla użytkownika root
- Ruch DNS Dokumentacja Palo Alto wyraźnie to potwierdza. DNS i HTTPS wykraczają poza dopuszczony ruch "do systemu + DHCP", co stanowi niezgodność z OPZ.
Wyjaśnienie: Według dokumentacji i dobrych praktyk, wymóg jest spełniony, ponieważ:
- Rozwiązanie w trybie izolacji blokuje ruch sieciowy endpointa z wyjątkiem kanału komunikacji z systemem zarządzającym oraz DHCP
- W praktyce technicznej połączenie do systemu wymaga utrzymania niezbędnych zależności tego kanału
- DNS i HTTPS są warstwami technicznymi niezbędnymi do utrzymania połączenia z systemem zarządzającym
- Wymóg OPZ "ruch do systemu" obejmuje mechanizmy potrzebne do jego zestawienia i utrzymania (DNS/FQDN, HTTPS/TLS)
Ocena:
1. Interpretacja celowościowa – OPZ wymaga blokady ruchu w celu ograniczenia mobilności atakującego w sieci. DNS/HTTPS do konsoli XDR nie umożliwiają komunikacji z innymi endpointami = cel spełniony
2. Dokumentacja producenta – Palo Alto explicite wskazuje: "halt all network access except for traffic to Cortex XDR". DNS/HTTPS są częścią "traffic to Cortex XDR"
3. Praktyczna konieczność – agent musi rozwiązać nazwę domenową konsoli (DNS) i ustanowić bezpieczne połączenie (TLS/HTTPS). Bez tego izolacja uniemożliwiłaby zarządzanie endpointem
4. Precedens techniczny – większość rozwiązań XDR/EDR dopuszcza warstwy protokołów niezbędne do komunikacji z konsolą
Zarzut nr 4: Ust. 65 OPZ – Usuwanie złośliwych makr Office Wymóg: "Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel." Zarzut: Cortex XDR nie posiada funkcji usuwania złośliwych makr z dokumentów Word/Excel. System oferuje:
- Blokowanie wykonania makr (Block)
- Raportowanie wykrycia makr (Report)
- Usuwanie/kwarantannę całego pliku (Search and Destroy) Brak funkcji selektywnego czyszczenia kodu VBA z dokumentu z pozostawieniem treści pliku. Dokumentacja producenta potwierdza, że działania reakcyjne są ograniczone do blokowania wykonania makra oraz usuwania całego pliku, nieoczyszczania dokumentu z makr.
Wyjaśnienie: Malware Prevention Profile blokuje wykonanie złośliwych makr w plikach Office (funkcja "Office Files with Macros Examination"). Dodatkowo Search and Destroy usuwa lub umieszcza w kwarantannie pliki uznane za złośliwe. Równoważna ochrona.
Ocena
1. Interpretacja funkcjonalna vs. literalna – celem wymogu jest eliminacja zagrożenia, nie - konkretna metoda. Blokada wykonania makr + usunięcie pliku = cel osiągnięty
2. Standard rynkowy – większość rozwiązań XDR/EDR (CrowdStrike, Microsoft Defender, SentinelOne) również nie oferuje selektywnego czyszczenia makr VBA, tylko blokadę lub usunięcie pliku
3. Przewaga bezpieczeństwa – usunięcie całego zainfekowanego pliku jest bezpieczniejsze niż próba czyszczenia VBA (ryzyko residuum złośliwego kodu)
4. Brak precyzji OPZ – wymóg nie wskazuje "z zachowaniem treści pliku" ani "bez usuwania dokumentu"
Zarzut nr 5: Ust. 70 OPZ – Automatyczne skanowanie USB Wymóg OPZ: "Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB."
Zarzut: Cortex XDR nie oferuje automatycznego, natychmiastowego skanowania pamięci masowej w momencie podłączenia nośnika do portu USB. System oferuje:
- Device Control – blokowanie dostępu do USB, generowanie alertów
- Periodic Scan – cykliczne skanowanie z opcją "Scan Removable Media Drives" (np. tygodniowo) Brak natywnej funkcji "scan on connect". Wymóg OPZ explicite wskazuje "natychmiast", co oznacza event-driven scan, nie scheduled scan.
Wyjaśnienie: Clockwise: Device Control pozwala kontrolować dostęp do urządzeń USB (blokowanie odczytu/zapisu, ograniczanie typów urządzeń, alerty). Periodic Scan z opcją Removable Media zapewnia równoważną ochronę. Prewencja (blokada) lepsza niż detekcja (scan).
Ocena:
1. Przewaga prewencji nad detekcją – Device Control blokujący USB default + allowlist to wyższy poziom

bezpieczeństwa niż skanowanie after-the-fact
2. Zero-trust model – blokada wszystkich USB z wyjątkiem zatwierdzonych urządzeń eliminuje zagrożenie u źródła
3. Interpretacja celu OPZ – celem jest ochrona przed malware z USB, co osiąga się skuteczniej przez blokadę niż scan
4. Brak zakazu alternatyw – OPZ nie stanowi "wyłącznie przez scan on-connect"
Zamawiający stoi na stanowisku, tak jak podkreślała wielokrotnie KIO w swoich wyrokach, że „In dubio pro performerem", czyli wszelkie niejednoznaczności w OPZ należy interpretować na korzyść wykonawcy składającego ofertę. Jeśli zamawiający chciał wykluczyć równoważne rozwiązania, powinien to jednoznacznie określić w OPZ, co potwierdzają orzeczenia wydane w sprawach KIO 1456/18, KIO 2234/19, KIO 987/21.
Oferta jest niezgodna z warunkami zamówienia tylko wtedy, gdy cel określony w OPZ nie może zostać osiągnięty. Jeśli Clockwise oferuje alternatywne metody realizacji tych samych celów (ochrona przed malware, izolacja zagrożeń, kontrola USB), niezgodność nie zachodzi, co potwierdza nietrafność zarzutu odwołującego, tj. art. 226 ust. 1 pkt 5 PZP.
Zamawiający zastosował art. 131 ustawy, wezwał Clockwise do wyjaśnień, otrzymał szczegółowe odpowiedzi potwierdzone dokumentacją producenta, dokonał weryfikacji merytorycznej. Trecom nie kwestionuje procedury, tylko ocenę merytoryczną.
Odrzucenie oferty tańszej o 3.224,52 zł z powodu niejasności interpretacyjnych byłoby nieproporcjonalne wobec celu postępowania (wybór najkorzystniejszej oferty). Szczególnie gdy druga oferta (Trecom) również była dostępna. Wybór oferty Trecom (nie narusza interesu publicznego, ale przedłuża postępowanie i opóźnia realizację krytycznego projektu bezpieczeństwa IT w sektorze medycznym (WUM).
Zamawiający, biorąc pod uwagę powyższe, a także uwzględniając następujące fakty, min. dotyczące zgodności z dokumentacją producenta (Palo Alto Networks), tj. brak sprzeczności, a także udzielenie wyczerpującej odpowiedzi na wezwanie zamawiającego przez wykonawcę, która kompleksowo wykazała spełnienie warunków opisanych w OPZ, powinno skutkować oddaleniem odwołania odwołującego w całości jako bezzasadnego.
20 marca 2026 r. przystępujący przedstawił pisemne stanowisko i wniósł o przeprowadzenie
dowodów z przedłożonych dokumentów.
Zarzut 1
Zarzut jest oczywiście bezzasadny. Oparty on został na nierzetelnej ocenie wyjaśnień złożonych przez przystępującego, nieznajomości rozwiązania zaoferowanego przez przystępującego oraz przedstawieniu błędnego rozumienia wymogu SWZ.
Jak wynika z wyjaśnień złożonych przystępującego, w żadnym ich miejscu nie wskazał on, wbrew twierdzeniom odwołującego, że w systemie Cortex XDR przeszukiwanie nie jest realizowane za pomocą API.
W odpowiedzi na punkt 3 zapytania zamawiającego, powołując się na konkretne postanowienia dokumentacji producenta, przystępujący wskazał w treści swoich wyjaśnień:
• „Rozwiązanie umożliwia przeszukiwanie danych telemetrycznych pod kątem IoC zarówno z poziomu konsoli (XQL), jak i z poziomu API [……]".
Dalej przystępujący wskazał w swoich wyjaśnieniach w jaki sposób realizowane jest przeszukanie ww. danych z poziomu tj. za pomocą API:
• „[…..] poprzez XQL Query APIs (Start XQL Query + pobranie wyników Get XQL Query Results / Stream)."
Powyższe wprost zatem zaprzecza twierdzeniom odwołującego.
Przystępujący równocześnie wskazał, że zastosowany w systemie Cortex XDR sposób realizacji ww. wymagania SWZ tj. przez XQL Query APIs (Start XQL Query + pobranie wyników Get XQL Query Results / Stream)" w żaden sposób ni oznacza braku jego spełnienia. Twierdzenia odwołującego w tym zakresie nie tylko nie zostały udowodnione, ale są również całkowicie bezzasadne.
W odniesieniu do stwierdzenia odwołującego, że w przypadku rozwiązania przystępującego:
„API służy tutaj tylko i wyłącznie do pobrania wszystkich danych, a przeszukiwanie jest realizowane w inny sposób";
wymaga zauważenia, że wymóg SWZ nie brzmi, jak chciałby tego odwołujący tj., aby API służyło do przeszukiwania danych, ale aby przeszukiwanie danych było możliwe z poziomu API. W przypadku rozwiązania przystępującego taka możliwość istnieje. Przeszukiwanie danych jest możliwe z poziomu API, a przyjęty w rozwiązania Cortex XDR sposób tego przeszukiwania jest zgodny z SWZ. Zamawiający zresztą nie określił w SWZ szczegółowego sposobu przeszukiwania identyfikatorów via API.
Przystępujący równocześnie wskazał, że użyte prze niego w złożonych wyjaśnieniach stwierdzenie: „tym samym przeszukiwanie „via API" jest realizowane w sposób równoważny, zgodny z dokumentacją producenta" nie oznaczało, że przystępujący oferuje inny sposób realizacji wymagania niż opisał to zamawiający. Zgodnie ze słownikiem języka polskiego słowo „równoważny" oznacza m.in. zgodny, taki sam, mający tę samą wartość i w tym znaczeniu przystępujący użył tego określenia tj., że przeszukiwanie via API odbywa się w sposób zgodny z wymogiem SWZ.
Przystępujący wniósł o przeprowadzenie dowodu z:

a) Wyjaśnień treści oferty (pismo z dnia 16.01.2026 r.) złożonych przez przystępującego (odpowiedź do punktu 3) – znajduje się w aktach postępowania;
b) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR-REST-API/XQL Query - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta („zarzut 1”);
na fakt, że zaoferowany przez przystępującego system Cortex XDR Cortex XDR umożliwia przeszukiwanie danych telemetrycznych pod kątem identyfikatorów IoC z poziomu API przez użycie funkcji: XQL Query APIs (Start XQL Query + pobranie wyników Get XQL Query Results / Stream), co realizuje wymóg z ust. 8 załącznika nr 2.1 do SWZ (OPZ) tj.:
„System musi przechowywać przez 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.”
Ad. zarzut nr 2
Istotą zarzutu opisanego w pkt III.b uzasadnienia odwołania jest twierdzenie odwołującego, że zaoferowany przez przystępującego system Cortex XDR nie spełnia poniższego wymagania określonego w ust. 10 pkt 1) lit. b załącznika nr 2.1 do SWZ (OPZ):
• system musi posiadać możliwość instalacji agenta m.in. dla systemu operacyjnego Microsoft Windows 10 dla architektury procesorów x86-64 i arm64.
Przystępujący stwierdził, że poniższe twierdzenie odwołującego:
• „ofertowany przez Clockwise system Cortex XDR nie ma możliwości instalacji agenta na systemie Windows 10 dedykowanym dla architektury procesora ARM64”
jest bezpodstawne, nierzetelne i jest wynikiem wybiórczej z jego strony interpretacji dokumentacji dotyczącej systemu Cortex XDR. Odwołujący nie przeanalizował całości dokumentacji producenta i oparł swój zarzut jedynie na swoich domysłach.
Przystępujący równocześnie w pełni podtrzymał złożone w treści wyjaśnień oferty oświadczenie, że wsparcie dla systemów operacyjnych Windows, w tym Windows 10 opartych na procesorach ARM, w tym ARM64 w oferowanym rozwiązaniu XDR jest dostępne.
Uznając za zbyteczne odnoszenie się do poszczególnych stwierdzeń odwołującego zawartych w treści odwołania, a rzekomo uzasadniających ten zarzut przystępujący wniósł o przeprowadzenie dowodu z:
c) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/9.0/Cortex-XDR-Agent-Release-Notes/Feature-Enhancements - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta („zarzut 2”)
oraz
d) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Compatibility-Matrix/Windows - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta „zarzut 2”)
na fakt, że dla wersji Cortex XDR Agent 9.0 istnieje wsparcie dla systemów operacyjnych Windows opartych na architekturze procesorów ARM64 oraz że środowisko Windows 10 znajduje się w zakresie kompatybilności Agenta Cortex XDR, zarówno w wersji 9.0 jak również dla wersji 9.1. oraz kolejnych wersjach.
Powyższe potwierdza, że ofertowany przez Clockwise system Cortex XDR ma możliwość instalacji agenta na systemie Windows 10 dedykowanym dla architektury procesora ARM64, co stanowi spełnienie wymogu SWZ;
Ad. zarzut nr 3
Istotą zarzutu opisanego w pkt III.c uzasadnienia odwołania jest twierdzenie Odwołującego, że zaoferowany przez Przystępującego system Cortex XDR nie spełnia poniższego wymagania określonego w ust. 34 załącznika nr 2.1 do SWZ (OPZ):
• „System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.”
Odwołujący stwierdza:
• „system Cortex XDR w trakcie trwania izolacji skompromitowanego endponita na serwerach Linux, poza połączeniami do systemu oraz protokołu DHCP, dopuszcza ruch DNS i HTTPS z siecią, co oczywiście wykracza poza dopuszczony warunkiem ruch do konsoli XDR.”
Przystępujący wskazał analogicznie jak w przypadku innych zarzutów odwołania, że powyższy zarzut jest oczywiście bezzasadny. Przystępujący w sposób jednoznaczny potwierdził w wyjaśnieniach treści oferty spełnienie przedmiotowego wymagania, wskazał bowiem:
• „[…..] rozwiązanie w trybie izolacji blokuje ruch sieciowy endpointa z wyjątkiem kanału komunikacji z systemem zarządzającym oraz DHCP.”
Powyższe stwierdzenie przystępujący oparł na wskazanym w wyjaśnieniach fragmencie dokumentacji producenta, gdzie czytamy:
• "When you isolate an endpoint, you halt all network access on the endpoint except for traffic to Cortex XDR."(tłum.

„Izolując punkt końcowy, zatrzymujesz cały dostęp do sieci na tym punkcie, z wyjątkiem ruchu do Cortex XDR.").
Należy stwierdzić, że powyższe jest jednoznacznym potwierdzeniem spełnienia wymogu SWZ:
• „System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany."
Wbrew twierdzeniom odwołującego dalsza część wyjaśnień przystępującego tj.:
•
„Jednocześnie wskazujemy, że w praktyce technicznej „połączenie do systemu" wymaga utrzymania niezbędnych zależności tego kanału DNS i HTTPS są warstwami technicznymi niezbędnymi do utrzymania połączenia z systemem zarządzającym. Wymóg OPZ dopuszcza ruch „do systemu", a więc obejmuje również mechanizmy potrzebne do jego zestawienia i utrzymania takie jak DNS/FQDN oraz HTTPS/TLS" w żaden sposób nie stoi w sprzeczności z ustaleniem że w trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.
Dopuszczenie przez producenta w trakcie trwania izolacji wybranych typów ruchu tj. m.in. DNS oraz wyjściowy HTTPS w żaden sposób nie oznacza, że dopuszczony jest ruch sieciowy poza połączeniem do systemu oraz protokołem DHCP. Z dokumentacji wprost bowiem wynika, że te typy ruchu tj. DNS oraz HTTPS są niezbędne do utrzymania połączenia z systemem zarządzającym, co zamawiający wprost dopuścił w SWZ („ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany").
Przystępujący wyjaśnił że sformułowanie SWZ „połączenia do systemu" należy rozumieć szerzej niż samo utrzymanie sesji — obejmuje ono również zależności warstwowe, bez których zestawienie oraz stabilne utrzymanie łączności z usługami chmurowymi nie byłoby możliwe.
Ruch DNS jest wymagany do prawidłowego rozwiązywania nazw FQDN usług po stronie chmury, co stanowi warunek nawiązania komunikacji pomiędzy agentem a konsolą. Z kolei HTTPS/TLS jest podstawowym, szyfrowanym kanałem transmisji wykorzystywanym do bezpiecznej komunikacji z systemem zarządzającym, w tym do przesyłania telemetrii, poleceń oraz potwierdzeń wykonania działań w ramach izolacji.
Przystępujący wniósł o przeprowadzenie dowodu z:
a) Wyjaśnień treści oferty (pismo z dnia 16.01.2026 r.) złożonych przez przystępującego (odpowiedź do punktu 2) – znajduje się w aktach postępowania;
e) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.x-Documentation/Isolate-an-endpoint - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta („zarzut 3")
na fakt, że zaoferowany przez przystępującego system Cortex XDR realizuje wymóg z ust. 34 załącznika nr 2.1 do SWZ (OPZ) tj.:
Ad. zarzut nr 4
Zarzut opisany w pkt III.d uzasadnienia odwołania oparty jest na twierdzeniu odwołującego, że zaoferowany przez przystępującego system Cortex XDR nie spełnia poniższego wymagania określonego w ust. 65 załącznika nr 2.1 do SWZ (OPZ):
• „Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel."
Istotą ww. zarzutu jest następujące stwierdzenie odwołującego (pkt 43 uzasadnienia odwołania):
• system nie dysponuje wymaganą przez zamawiającego funkcjonalnością usunięcia wyłącznie złośliwego kodu makra z dokumentu z pozostawieniem niezmienionej resztę zawartości pliku Word/Excel, tak jak zostało to opisane w ust. 65 OPZ.
Przystępujący wskazał, że powyższy zarzut jest oczywiście bezzasadny.
O bezzasadności ww. zarzutu świadczy już sama okoliczność, w której oparty jest on na interpretacji ww. wymagania pozostającej w sprzeczności z jego faktyczną treścią. Zdaniem odwołującego z cytowanego wyżej wymagania z ust. 65 załącznika nr 2.1 do SWZ wynika jakoby agent musiał mieć możliwość usunięcia wyłącznie złośliwego kodu makra z dokumentu z pozostawieniem niezmienionej reszty zawartości pliku Word/Excel. Przystępujący podkreślił, że w treści przedmiotowego wymagania nie pojawiają się sformułowania użyte przez odwołującego tj. „wyłącznie złośliwego kodu", „z dokumentu" oraz „z pozostawieniem niezmienionej reszty zawartości pliku".
Określając wymóg „Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel" zamawiający nie narzucił sposobu jego realizacji tj. sposobu usunięcia złośliwych makr. Istotą wymagania jest to, aby Agent miał możliwość usunięcia złośliwych makr wykrytych w plikach Word/Excel. Agent w rozwiązaniu zaoferowanym przez Przystępującego ma taką możliwość, tj. wykryte w plikach Word/Excel złośliwe makra mogą być usunięte przez usunięcie całego pliku Word/Excel, w którym wykryto złośliwe makro. Taki sposób realizacji wymagania SWZ nie jest sprzeczny z jego treścią.
Wymóg SWZ nie wskazuje, że jedynym sposobem usunięcia złośliwych makr jest usunięcie samego kodu makra z

dokumentu, a po jego usunięciu dokument musi pozostać w niezmienionej treści.
Przystępujący wniósł o przeprowadzenie dowodu z:
f) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.x-Documentation/Add-Quick-Actions-commands-and-scripts - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta („zarzut 4")
na fakt, że zaoferowany przez przystępującego system Cortex XDR wspiera analizę i blokowanie złośliwych makr w plikach Microsoft Office w ramach profili prewencji (Office files with macros examination, tryb Block/Report), a także działania reakcyjne/remediacyjne na artefaktach, takie jak kwarantanna lub usunięcie pliku (z wykorzystaniem wbudowanych automatyzacji), co oznacza, że realizuje wymóg z ust. 65 załącznika nr 2.1 do SWZ (OPZ).
Ad. zarzut nr 5
Istotą zarzutu opisanego w pkt III.e uzasadnienia odwołania jest twierdzenie odwołującego, że zaoferowany przez przystępującego system Cortex XDR nie spełnia poniższego wymagania określonego w ust. 70 załącznika nr 2.1 do SWZ (OPZ):
• „Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB."
O bezzasadności ww. zarzutu świadczy już sama okoliczność, w której oparty jest on na interpretacji ww. wymagania pozostającej w sprzeczności z jego faktyczną treścią. Zdaniem odwołującego bowiem skanowanie, o którym mowa w ww. wymaganiu ma mieć na celu automatyczne wyzwalanie skanu wirusowego, co przecież nie wynika z treści tego wymagania.
Przystępujący zwrócił uwagę, że wymóg z ust. 70 załącznika nr 2.1 do SWZ wskazuje na konieczność automatycznego skanowania pamięci masowej po jej podłączeniu do portu USB natomiast nie określa rodzaju/zakresu/efektu tego skanowania. Nie jest zatem zgodne z treścią SWZ twierdzenie odwołującego, że ww. automatyczne skanowanie ma mieć na celu automatyczne wyzwalanie skanu wirusowego.
W przypadku rozwiązania zaoferowanego przez przystępującego bezpieczeństwo w ww. obszarze realizuje się dwutorowo:
(1) przez natychmiastowe rozpoznanie i kontrolę podłączonego urządzenia oraz
(2) przez kontrolę i analizę plików w momencie ich użycia lub w ramach skanów planowych / na żądanie.
Cortex XDR zapewnia funkcję Device Control, która pozwala wykrywać i klasyfikować podłączane urządzenia USB (w tym pamięci masowe) oraz egzekwować polityki dopuszczenia bądź blokowania nośników (np. tylko zaufane/zaakceptowane urządzenia), co stanowi automatyczną reakcję „natychmiast po podłączeniu" i pozwala ograniczyć ryzyko jeszcze zanim dojdzie do skopiowania lub uruchomienia plików z nośnika. Te informacje możemy znaleźć w dokumentacji Producenta dostępnej pod linkiem poniżej:
Przystępujący wniósł o przeprowadzenie dowodu z:
g) dokumentacji producenta zawartej na stronie https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-5.x-Documentation/Device-control - w załączeniu: wydruk zrzutu ekranu dot. kluczowego stwierdzenia producenta („zarzut 5")
na fakt, że zaoferowany przez przystępującego system Cortex XDR zawiera funkcję agenta Device Control, która polega na automatycznym skanowaniu pamięci masowej natychmiast po jej podłączeniu, gdzie skanowanie to pozwala automatycznie wykrywać i klasyfikować podłączane urządzenia USB (w tym pamięci masowe) oraz egzekwować polityki dopuszczenia bądź blokowania nośników (np. tylko zaufane/zaakceptowane urządzenia), co oznacza, że realizuje wymóg z ust. 70 załącznika nr 2.1 do SWZ (OPZ).
Stan faktyczny:
KIO na podstawie dokumentacji postępowania o udzielenie zamówienia oraz dowodów złożonych przez odwołującego i przystępującego ustaliła, co następuje:
W SWZ zamawiający postanowił:
III. Opis przedmiotu zamówienia
6. W sytuacjach, gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do norm, ocen technicznych, specyfikacji technicznych i systemów referencji technicznych, Zamawiający dopuszcza rozwiązania równoważne opisywanym w każdej takiej normie, ocenie technicznej, aprobacie, specyfikacji technicznej, systemie referencji technicznych spełniające wymagania określone w opisie przedmiotu zamówienia.
7. W sytuacjach, gdy Zamawiający opisuje przedmiot zamówienia poprzez odniesienie się do wymagań dotyczących wydajności lub funkcjonalności Zamawiający dopuszcza rozwiązania równoważne opisywanym, zgodne z Polską Normą przenoszącą normę europejską, normami innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszącymi normy europejskie, z europejską ocena techniczną, ze wspólną specyfikacją techniczną, z normą międzynarodową lub z systemem referencji technicznych ustanowionym przez europejski organ normalizacyjny, jeżeli te normy, oceny techniczne, specyfikacje i systemy referencji technicznych spełniają wymagania dotyczące wydajności lub

funkcjonalności określone przez Zamawiającego.
XI. PRZEDMIOTOWE ŚRODKI DOWODOWE
W celu potwierdzenia, że oferowane dostawy spełniają określone przez Zamawiającego wymagania oraz cechy, Zamawiający nie żąda złożenia wraz z ofertą przedmiotowych środków dowodowych.
XII. KRYTERIA OCENY OFERT ORAZ ICH ZNACZENIE ORAZ SPOSÓB OCENY OFERT
Zamawiający w Pakietach 1 - 5 odstąpił od zastosowania kryterium ceny o wadze nie przekraczającej 60%, zgodnie z zasadą wyrażoną w art. 246 ust. 2 ustawy Pzp, kierując się optymalizacją jakości oferowanych produktów w korelacji z ich wartością.
Zamawiający jednocześnie wyjaśnia, że w Opisie Przedmiotu Zamówienia (Załączniki nr 2.1-2.5 do SWZ) określił szczegółowe wymagania techniczne i funkcjonalne, będące wyznacznikiem jakości właściwej dla określonego segmentu systemów, odnoszące się do głównych cech funkcjonalnych pozostających w ofercie spośród kręgu Wykonawców oferujących tego typu rozwiązania.
XXII. ODRZUCENIE OFERTY
1. Zamawiający odrzuci ofertę, w przypadku zaistnienia okoliczności, o których mowa w art. 226 ust. 1 ustawy.
Załącznik nr 2.1-zmiana
-wniosek 4114/APU/2025
OPIS PRZEDMIOTU ZAMÓWIENIA
8.System musi przechowywać przez 365 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.
10.System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
1)Microsoft:
b)Windows 10 (x86-64 oraz arm64)
34.System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.
65.Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.
70.Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB.
Wyjaśnienia treści SWZ:
Pytanie nr 2
Punkt:
8. System musi przechowywać przez 365 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.
Pytanie:
Czy przez „przechowywanie i przeszukiwanie IoC" Zamawiający rozumie wyłącznie dane dotyczące alertów bezpieczeństwa, czy również pełną telemetrię z monitorowanych stacji roboczych i serwerów, obejmującą aktywności niebędące alertami?
Czy Zamawiający dopuszcza, aby system umożliwiał przechowywanie i przeszukiwanie danych w okresie 186 dni lub 30 dni, w zależności od rodzaju danych oraz licencjonowania?
Odpowiedź na pytanie nr 2:
Zamawiający dokonuje zmiany Załącznika 2.1 do SWZ, poprzez nadanie brzmienia w ust. 7 i 8:
7. System musi przechowywać informacje o alarmach i incydentach co najmniej przez 90 30 dni.
8. System musi przechowywać przez ~~365~~ 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.
Odpowiedź na pytanie nr 17:
Tak, Zamawiający uzna ofertę za spełniającą wymagania, jeżeli system XDR nie będzie zapewniał wsparcia dla wycofanych lub obecnie wycofywanych systemów operacyjnych, jednocześnie wspierając nowsze wersje wymienionych systemów.
Zamawiający dokonuje zmiany Załącznika 2.1 do SWZ, poprzez nadanie brzmienia w ust. 10:
10. System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
1) Microsoft:
a) Windows 7 SP1
b) Windows 10 (x86-64 oraz arm64)
c) Windows 11 (x86-64 oraz arm64)

d) Server 2008 R2 SP1
e) Server 2012 i 2012 R2
f) Server 2016 i Server Core 2016
g) Server 2019 i Server Core 2019
h) Server 2022 i Server Core 2022
2) Linux
a) CentOS ~~6, 7~~ i 8
b) Debian ~~9~~,10, 11 i 12
c) Oracle Linux ~~6~~, 7, 8 i 9
d) Red Hat Enterprise Linux ~~6~~, 7, 8 i 9
~~e) Red Hat Enterprise CoreOS 4~~
f) Rocky Linux 8 i 9
g) SUSE ~~11~~, 12 i 15
h) Ubuntu ~~14, 16~~, 18, 20 i 22
3) Apple macOS
~~a) macOS Monterey 12~~
~~b) macOS Ventura 13~~
c) macOS Sonoma 14
4) Apple iOS 18x lub nowszy ~~15.x, 16.x i 17.x~~
5) Android 12.x, 13.x i 14.x
Oferta przystępującego:
2.Składając ofertę w postępowaniu o udzielenie zamówienia publicznego, oferuję wykonanie zamówienia - Dostawę z uruchomieniem narzędzi do zarządzania bezpieczeństwem klasy XDR:
Producent (marka) Palo Alto Networks(Należy podać)
Nazwa, wersja Cortex XDR Pro: 1. PAN-XDR-PRO-GB; 2. PAN-XDR-ADV-EP; 3. PAN-XDR-FRNS (Należy podać)
spełniającego wymagania określone w Opisie Przedmiotu Zamówienia, stanowiącym Załącznik nr 2.1 do SWZ
6. Oświadczam, że oferowany system spełnia wszystkie wymagania określone w Załączniku nr 2.1 do SWZ – Opis Przedmiotu Zamówienia.
12 stycznia 2026 r. zamawiający skierował wezwanie w trybie arrt. 223 ust. 1 do przystępującego o treści:
Zamawiający powziął informację, wskazującą na niezgodność oferty z warunkami zamówienia.
Mając na uwadze powyższe Zamawiający zwraca się o wyjaśnienie w poniższym zakresie:
1) Zgodnie z p. 10.1.b. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR - zmiana
„System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
1) Microsoft:
a) Windows 7 SP1
b) Windows 10 (x86-64 oraz arm64)”
Zgodnie z dokumentacją do rozwiązania Cortex XDR firmy Palo Alto zamieszczoną na stronieagent Cortex XDR nie jest dostępny dla Windows 10 dla architektury arm64.
W tabeli dostępnych systemów operacyjnych uwidocznione są tylko wersje Windows 10 dla architektury x86-64.
W tym miejscu zamawiający zamieścił print screen z powołanej strony producenta.
Architektura arm64 jest wspierana tylko dla Windows 11, co jest wprost wskazane w tabeli uwidocznionej w dokumentacji na podanej powyżej stronie Palo Alto.
Tu także zamieszczono print screen
Powyższe wskazuje, że rozwiązanie Cortex XDR nie spełnia wymagania 10.1.b postawionego przez Zamawiającego w Załączniku 2.1 Opis Przedmiotu Zamówienia.
2) Zgodnie z p. 34. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR - zmiana
„System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany
Zgodnie z dokumentacją do rozwiązania Cortex XDR firmy Palo Alto zamieszczoną na stronie
https://docs-cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-4.x-Documentation/Initiate-a-Live-Terminal-session
w sekcji „Isolate an endpoint” wskazane jest, iż w przypadku stosowania rozwiązania Cortex XDR izolowana stacja końcowa zachowuje połączenie z konsolą zarządzającą systemu oraz dostęp do usług DNS, a dodatkowo na serwerach Linux dopuszcza wychodzące połączenia HTTPS dla procesów użytkownika root.
Znajduje to swoje odzwierciedlenie w zapisie

Tu zamieszczono print screen

Tłumaczenie:

„Wyizolowanie punktu końcowego

Gdy izolujesz punkt końcowy, dochodzi do zablokowania dostępu do sieci z tego urządzenia końcowego z wyjątkiem ruchu do Cortex XDR. Służy to temu, aby skompromitowane urządzenie końcowe nie miało możliwości komunikacji z innymi punktami końcowymi, ograniczając mobilność atakującego w Twojej sieci. Po otrzymaniu przez agenta instrukcji by izolować urządzenie końcowe i wykonaniu tej akcji, Cortex XDR wskazuje status ***Izolowany****. Aby zapewnić, że urządzenie końcowe pozostanie w izolacji, w czasie jej trwania dla izolowanych urządzeń nie są dostępne aktualizacje oprogramowania agenta.*

Po izolacji punkt końcowy nadal pozwala na:

• Ruch wychodzący DHCP i HTTPS dla użytkownika root

• Ruch DNS”

Stoi to w sprzeczności z wymaganiem 34, zgodnie z którym Zamawiający wskazał, że cały ruch poza połączeniem do systemu oraz protokołem DHCP musi zostać zablokowany.

Jednocześnie nie można uznać, że ruch DNS czy HTTPS jest ruchem kierowanym wyłącznie do konsoli zarządzającej systemu XDR.

3) Zgodnie z p. 8. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR – zmiana

„System musi przechowywać przez 365 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.”

Zgodnie z dokumentacją do rozwiązania Cortex XDR firmy Palo Alto zamieszczoną na stroniesystem ten nie daje możliwości przeszukiwania indykatorów za pośrednictwem API.

4) Zgodnie z p. 77. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR - zmiana

„Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:

1) Utworzenie nowego procesu i zakończenie procesu

2) Operacje na socketach sieciowych dla TCP i UDP

3) Operacje na plikach

4) Zdarzenia z event logu dotyczącego uwierzytelnienia.

5) Operacje na rejestrze (tylko systemy Windows)”

Zgodnie z dokumentacją do rozwiązania Cortex XDR firmy Palo Alto zamieszczoną na stronieDocumentation/Endpoint-data-collection?tocId=0d1SBdboAHhrDkltBsIZMw

zbieranie i wysyłanie danych telemetrycznych z systemów Linux i MacOS w zakresie wymagania 77.3 oraz 77.4 wymaga zastosowania dedykowanego dodatku licencjonowanego per urządzenie końcowe, pod nazwą Extended Threat Hunting (dalej opisywany również jako XTH).

Wymóg związany z koniecznością „dozbrojenia” systemu w dodatek XTH jest uwidoczniony zarówno w sekcji dla MacOS jak i dla Linux (we wskazanej dokumentacji).

To zamawiający zamieścił print screen

Dla Maos

Dla Linux

Zdanie „Requires XTH add-on” należy tłumaczyć jako „Wymaga dodatku XTH” XTH jest opcją dodatkowo licencjonowana przez Palo Alto, nie jest on wliczony standardowo w koszt licencji XDR, a także jako dodatek ma swoją pozycję cennikową (tzw. part-number, opis oraz cenę za każde urządzenie końcowe)

PAN-XDR-XTH Extended Threat Hunting (enhanced visibility) add-on for Cortex XDR ProEP/Cloud (price per Endpoint Includes 30 days of data retention.

Tłumacząc opis tej licencji możemy przeczytać, że jest to „Dodatek Extended Threat Hunting (zwiększona widoczność) dla Cortex XDR ProEP/Cloud (cena za punkt końcowy). Obejmuje 30 dni retencji danych.”

Kluczowym jest tutaj jednoznaczne wskazanie w opisie, że jest to element dodatkowy względem Cortex XDR ProEP/Cloud (co jednocześnie potwierdza, że nie jest on wliczony w cenę licencji Cortex XDR Pro i objęty jednym i tym samym kodem produktu)

Zgodnie ze złożonym Formularzem Ofertowym firma Clockwise jako Wykonawca zadeklarowała zaoferowanie/wolę dostarczenia Zamawiającemu następujących licencji (podajemy numery katalogowe Palo Alto wraz z opisem):

PAN-XDR-PRO-GB Cortex XDR Pro for daily ingested GB. Includes 30 days of ingested data retention, 180 days of alert and incidents retention and standard success

PAN-XDR-ADV-EP Cortex XDR Pro for 1 endpoint, includes 30 days of data retention and standard success

PAN-XDR-FRNS Annual Forensics add-on for 1 Cortex XDR endpoint, includes 30 days of data retention
Nie ma wśród nich licencji na dodatek XTH, którego brak powoduje, że zaoferowane przez firmę Clockwise rozwiązanie Cortex XDR nie spełnia wymagania 77 postawionego przez Zamawiającego w Załączniku 2.1 Opis Przedmiotu Zamówienia.
Wyjaśnienia w powyższym zakresie należy złożyć, w terminie do dnia 16.01.2026 r.
Przystępujący przedstawił następujące wyjaśnienia:
Odpowiedź do punktu 1:
Zgodnie z p. 10.1.b. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR – zmiana.
„System musi posiadać możliwość instalacji agenta na co najmniej następujących systemach operacyjnych:
1) Microsoft: Windows 7 SP1
Windows 10 (x86-64 oraz arm64) ”
Powołując się na dokumentacje Producenta, opisujące najnowsze aktualizacje oprogramowania Cortex XDR Agent w wersji 9.0,:
informuje, iż aktualnie wsparcie dla systemów operacyjnych Windows opartych na procesorach ARM w oferowanym rozwiązaniu XDR jest dostępne. Tu zamieścił fragment dokumentacji zaznaczając XDR Agent for Windows on ARM64 Extend the industry leading prevention and detection capabilities of Cortex XDR to Windows endpoints running on ARM processors.
Odpowiedź do punktu 2:
Zgodnie z p. 34. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR - zmiana
„System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany” Powołując się na dokumentację Producenta, dostępną w poniższej dokumentacji:
Według naszej wiedzy, dobrych praktyk i naszego doświadczenia związanego z wdrażanie rozwiązań Cortex XDR, wymóg „w trakcie izolacji cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany” jest spełniony, ponieważ rozwiązanie w trybie izolacji blokuje ruch sieciowy endpointa z wyjątkiem kanału komunikacji z systemem zarządzającym oraz DHCP. W dokumentacji znajduje się zapis "When you isolate an endpoint, you halt all network access on the endpoint except for traffic to Cortex XDR."(tłum. „Izolując punkt końcowy, zatrzymujesz cały dostęp do sieci na tym punkcie, z wyjątkiem ruchu do Cortex XDR.”).
Jednocześnie wskazujemy, że w praktyce technicznej „połączenie do systemu” wymaga utrzymania niezbędnych zależności tego kanału DNS i HTTPS są warstwami technicznymi niezbędnymi do utrzymania połączenia z systemem zarządzającym. Wymóg OPZ dopuszcza ruch „do systemu”, a więc obejmuje również mechanizmy potrzebne do jego zestawienia i utrzymania takie jak DNS/FQDN oraz HTTPS/TLS.
Odpowiedź do punktu 3:
Zgodnie z p. 8. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR – zmiana
„System musi przechowywać przez ~~365~~ 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.”
Powołując się na dokumentację Producenta dostępną na poniższej stronie:
Rozwiązanie umożliwia przeszukiwanie danych telemetrycznych pod kątem IoC zarówno z poziomu konsoli (XQL), jak i z poziomu API poprzez XQL Query APIs (Start XQL Query + pobranie wyników Get XQL Query Results / Stream). Tym samym przeszukiwanie „via API” jest realizowane w sposób równoważny, zgodny z dokumentacją producenta.
Tu zamieścił Get XQL Query Results zaznaczając Get XQL Query Results Stream
Odpowiedź do punktu 4:
Zgodnie z p. 77. Załącznika 2.1 Opis Przedmiotu Zamówienia XDR - zmiana
„Agent dla systemów Windows, MacOS i Linux musi zbierać i wysyłać do systemu co najmniej następujące dane telemetryczne:

1) Utworzenie nowego procesu i zakończenie procesu
2) Operacje na socketach sieciowych dla TCP i UDP
3) Operacje na plikach
4) Zdarzenia z event logu dotyczącego uwierzytelnienia.
5) Operacje na rejestrze (tylko systemy Windows)”

W zapytaniu OPZ, Zamawiający nie wskazał wymogu podawania wszystkich kodów dostarczanego rozwiązania oraz kodów wszystkich dodatków licencyjnych.
Oświadczamy, że dodatek licencyjny:
PAN-XDR-XTH Extended Threat Hunting (enhanced visibility) add-on for Cortex XDR ProEP/Cloud (price per Endpoint

Includes 30 days of data retention - został uwzględniony w złożonej przez nas ofercie, a dostarczone rozwiązanie w pełni spełnia wymagania funkcjonalne i techniczne opisane przez Zamawiającego w OPZ w tym zakresie.
Dowody przystępującego:
- strona
„Pobieranie wyniku wykonywanego zapytania API XQL
Uwaga: Ten punkt końcowy działa tylko w przypadku zapytań XQL zainicjowanych przez /public_api/v1/xql/start_xql_query/.
Maksymalny rozmiar zestawu wyników to 1000. API nie obsługuje stronicowania, dlatego można ustawić wartości określające ograniczenie rozmiaru wyników i sposób oczekiwania na wyniki. Aby wyświetlić odpowiedzi zawierające więcej niż 1000 wyników, należy wywołać funkcję **get XQL Query results Stream**"
- strona
„Agent XDR dla systemu Windows na procesorach ARM64 Jako wiodący w branży rozszerzamy możliwości Cortex XDR, dla zapobiegania i wykrywania, na urządzeniach końcowych opartych o Windows na procesorach ARM"
- strona
„Wersja Enterprise jest testowana pod kątem kompatybilności. O ile nie zaznaczono inaczej, należy założyć, że **wszystkie wersje są również kompatybilne"**
- strona
„Izolując punkt końcowy, zatrzymujesz cały dostęp do sieci na tym punkcie, z wyjątkiem ruchu do Cortex XDR."
- strona
„Kiedy izolujesz urządzenie końcowe nadal dostępny jest:
•Ruch wychodzący DHCP i HTTPS dla użytkownika root
•Ruch DNS"
- strona
"Dodawanie szybkich akcji, poleceń i skryptów do podręczników umożliwia automatyzację powtarzalnych zadań i wykonywanie niestandardowych akcji w celu zwiększenia efektywności i usprawnienia procesów przepływu pracy"
- strona
„Kontrola urządzeń.
Domyślnie wszystkie zewnętrzne urządzenia USB i Bluetooth mogą łączyć się z Cortex XDR na urządzeniach końcowych z systemem Windows i macOS, a także dozwolone są wszystkie zadania drukowania. Aby chronić urządzenia końcowe przed podłączaniem się do urządzeń wymiennych, takich jak dyski twarde, napędy CD-ROM, stacje dyskietek, urządzenia Bluetooth i inne urządzenia przenośne, które mogą zawierać złośliwe pliki, Cortex XDR zapewnia kontrolę urządzeń. Można również blokować różne typy zadań drukowania.
Za pomocą kontroli urządzeń można:
•(Windows i macOS) Zablokować wszystkie obsługiwane urządzenia podłączone przez USB dla grupy urządzeń końcowych.
•(Windows i macOS) Zablokować po typie urządzenia USB, ale dodać do dozwolonej listy konkretnego producenta, który będzie dostępny z urządzenia końcowego.
•(Windows i macOS) Zablokować połączenia z klasycznymi urządzeniami Bluetooth lub usługami Bluetooth o niskim poborze energii. Są to dwa różne protokoły Bluetooth używane do połączeń bezprzewodowych o krótkim zasięgu."
- strona
„Oprócz blokowania uruchamiania złośliwego oprogramowania agent Cortex XDR może skanować punkty końcowe Windows, Mac i Linux oraz podłączone dyski wymienne w poszukiwaniu uśpionego złośliwego oprogramowania, które nie podejmuje aktywnych prób
- strona
"Sprawdź pliki pakietu Office na dyskach sieciowych
•Włącz
•Wyłącz
„Możesz włączyć agenta Cortex XDR w celu sprawdzenia plików Microsoft Office na dyskach sieciowych, gdy zawierają one makro próbujące się uruchomić."
- oświadczenie przedstawiciela PALOALTO z 19 marca 2026 r.:
Działając w imieniu PaloAlto Networks potwierdzam, że system Cortex XDR spełnia wszystkie wymagania określone w dokumentacji technicznej „Opis Przedmiotu Zamówienia" dla ww. Zamówienia, w tym:
1. Pkt 8. OPZ - System musi przechowywać przez 180 dni i umożliwiać przeszukiwanie z konsoli i via API co najmniej następujące typy indykatorów (ang. Indicators of Compromise): hashe SHA256 i MD5, adresy IPv4 i IPv6 oraz nazwy domenowe domena.

2. Pkt 10. (10.1. lit. b) OPZ System musi posiadać możliwość instalacji agenta dla systemu Windows 10 (x86-64 oraz arm64).
3. Pkt. 34 OPZ - System musi umożliwiać zdalną izolację sieciową endpointa. W trakcie trwania izolacji sieciowej cały ruch sieciowy z wyjątkiem połączenia do systemu oraz protokołu DHCP musi zostać zablokowany.
4. Pkt 65. OPZ - Agent musi posiadać możliwość usuwania złośliwych makr wykrytych w plikach Microsoft Word i Microsoft Excel.
5. Pkt. 70. OPZ - Agent musi automatycznie wykonywać skanowanie pamięci masowej natychmiast po jej podłączeniu do portu USB.

Rozważania Krajowej Izby Odwoławczej (KIO):

KIO dopuściła Clockwise Spółka z ograniczoną odpowiedzialnością Spółka Komandytowa z siedzibą w Warszawie, ul. Puławska 405A w charakterze uczestnika postępowania.

KIO nie dopatrzyła się okoliczności mogących skutkować odrzuceniem odwołania na podstawie art. 528 ustawy.

KIO oceniła, że odwołujący wykazał przesłankę materialnoprawną dopuszczalności odwołania, o której mowa w art. 505 ust. 1 ustawy.

Odwołanie należy oddalić. Zgodnie z rozdziałem III pkt. 7 SWZ zamawiający dopuścił rozwiązania równoważne opisanym przez siebie funkcjonalnościom, co oznacza, że zamawiający wbrew stanowisku odwołującego pozwalał na powoływanie się na rozwiązania równoważne.

Odnosząc się do niezgodności treści oferty przystępującego z pkt. 8 OPZ i brakiem możliwości przeszukiwania via API, to KIO uważa, że wymóg postawiony przez zamawiającego nie był jednoznaczny i mógł być zrozumiany tak jak to prezentuje odwołujący, czyli przeszukiwanie miało się odbywać z konsoli i przeszukiwanie miało się odbywać przez API. W ocenie KIO jednak ten wymóg można było również odczytać w ten sposób, że przeszukiwanie miało odbywać się łącznie przez API i z poziomu konsoli. Co do tego drugiego sposobu rozumienia wymogu, to w ocenie KIO, ze stanowiska odwołującego wynika, że ofertowana przez przystępującego usługa go spełnia. Odwołujący wskazuje, że API dostarcza wyniki, a konsola je przeszukuje. Bez dostarczenia wyników przez API nie doszłoby do ich przeszukania, więc łącznie przeszukanie następuje z konsoli i via API. Nadto według KIO z dokumentacji producenta wynika, że dla wyświetlenia więcej niż 1000 wyników należy wywołać funkcję get XQL Query results Stream, co w ocenie KIO przez użycie w funkcji słowa Query (czyli zapytania) wskazuje na możliwość parametryzacji otrzymywanych wyników, a w konsekwencji realizację wymogu przeszukania. Na ten sposób wskazują wyjaśnienia przystępującego składane tak zamawiającemu jak i w piśmie procesowym.

Co do wymogu instalacji agenta dla systemu Windows 10 dla arm64, to w ocenie KIO ponownie SWZ w tym zakresie nie była precyzyjna, bo o ile zamawiający w pkt 10 faktycznie wymienił Windows 10, to jednak udzielając odpowiedzi na pytania wykonawców odpowiedział „Tak, Zamawiający uzna ofertę za spełniającą wymagania, jeżeli system XDR nie będzie zapewniał wsparcia dla wycofanych lub obecnie wycofywanych systemów operacyjnych, jednocześnie wspierając nowsze wersje wymienionych systemów." Dla Windows 10 wsparcie zakończyło się 14 października 2025 r. Zamawiający udzielił wyjaśnienia, że uzna za spełniającą wymagania taką ofertę, która zapewni wsparcie dla nowszych wersji wymienionych systemów. Niewątpliwie usługa przystępującego dla Windows 11, co nie było sporne między stronami, wymóg wsparcia dla arm64. Zatem w świetle takich wyjaśnień zamawiającego oferta przystępującego winna była być uznana, za zgodną z SWZ.

Odnośnie do pkt 34 OPZ i ruchu sieciowego po DNS i HTTPS, to w ocenie KIO odwołujący nie wykazał, że nie jest t dopuszczony przez zamawiającego wyjątek „połączenia do systemu". Przystępujący twierdził konsekwentnie, że dla komunikacji zarządczej dla systemu Cortex utrzymywanie tego ruchu jest niezbędne. Niewątpliwie zamawiający dopuścił ruch w zakresie połączenia do systemu, a odwołujący, poza twierdzeniami, nie przedstawił dowodu, że ruch DNS i ruch HTTPS nie są niezbędne dla połączenia do systemu oferowanego przez przystępującego. Odwołujący nie wnioskował także w tym zakresie o przeprowadzenie dowodu z opinii biegłego. Z tego względu zarzut należało uznać za nieudowodniony.

W zakresie pkt. 65 OPZ, to KIO podziela stanowisko zamawiającego i przystępującego, co do tego, że zamawiający nie określił sposobu usuwania złośliwych makr wykrytych w plikach. W ocenie KIO można było ten wymóg rozumieć zarówno jako usunięcie całych plików wraz ze znajdującymi się w nich złośliwymi makrami, jak i wyizolowanie złośliwego makra w pliku i usunięcie go z pozostawieniem pozostałej części pliku. Rację należy przyznać przystępującemu, że to postanowienie nie brzmi usuwanie złośliwych makr z pliku, ale usuwanie złośliwych makr wykrytych w plikach, co oznacza, że obie metody mogły być zastosowane i spełniały funkcjonalność oczekiwaną przez zamawiającego. Zamawiający wskazał tu także na to, że funkcji usuwania makr z plików Microsoft nie realizuje nawet oprogramowanie producenta Microsoft – Microsoft Defender. Wydawałoby się logiczne, że twórca oprogramowania powinien dostarczać narzędzie umożliwiające usuwanie zagrożeń z własnych plików, bez uszkadzania tych plików w pozostałej części.

Jeśli chodzi o pkt. 70 OPZ, to w ocenie KIO odwołujący zrozumiał przedmiotowy wymóg szerzej od jego literalnego

brzmienia, bowiem w odwołaniu wskazuje na skanowanie wirusowe, podczas, gdy w pkt. 70 mowa jest wyłącznie o automatycznym skanowaniu pomięci masowej, ale bez określania celu tego skanowania. Odwołujący przyznał, że Cortex XDR funkcje kontrolne realizuje za pomocą Device Control. Przy zastosowaniu tej kontroli można zablokować wszystkie obsługiwane urządzenia podłączone przez USB, zablokować po typie urządzenia USB, ale dodać z dozwolonej listy konkretnego producenta, można zablokować połączenia z klasycznymi urządzeniami Bluetooth i usługami Bluetooth. Można także blokować różne typy zadań do drukowania. Z przedstawionych tłumaczeń wynika także, że „Oprócz blokowania uruchamiania złośliwego oprogramowania agent Cortex XDR może skanować punkty końcowe Windows, Mac i Linux oraz podłączone dyski wymienne w poszukiwaniu uśpionego złośliwego oprogramowania, które nie podejmuje aktywnych prób". W ocenie KIO to świadczy o wykonywaniu automatycznego skanowania.

W ocenie KIO, część zarzutów wynikała z różnic w możliwym rozumieniu SWZ, a część nie została udowodniona. Aby mogło dojść do odrzucenia oferty wykonawcy na podstawie art. 226 ust. 1 pkt 5 ustawy niezgodność jego oferty z warunkami zamówienia musi być jednoznaczna i niebudząca wątpliwości. Zdaniem KIO z takiej jednoznaczności i braku wątpliwości, w tym przypadku, nie można było stwierdzić. To spowodowało oddalenie odwołania.

O kosztach postępowania odwoławczego orzeczono na podstawie art. 574 i 575 ustawy, tj. stosownie do wyniku postępowania, z uwzględnieniem postanowień Rozporządzenia Prezesa Rady Ministrów w sprawie szczegółowych rodzajów kosztów postępowania odwoławczego, ich rozliczania oraz wysokości i sposobu pobierania wpisu od odwołania z dnia 30 grudnia 2020 r. (Dz.U. z 2020 r. poz. 2437) na podstawie par. 8 ust. 2 pkt. 1 cyt. rozporządzenia zaliczając w poczet kosztów koszty wpisu, wydatki pełnomocnika odwołującego i koszty jego dojazdu. Skoro zarzuty odwołania nie potwierdziły się, żaden z zaliczonych kosztów odwołującego nie podlegał rozliczeniu. Zamawiający wnosił o zasądzenie kosztów wydatków pełnomocnika w wysokości dowiedzionej fakturą, zatem KIO nakazała odwołującemu zwrot na rzecz zamawiającego tych poniesionych kosztów.

Przewodnicząca: ……