Sygn. akt: KIO 3098/24

WYROK

Warszawa, dnia 20 września 2024 r.

Krajowa Izba Odwoławcza - w składzie:

Przewodnicząca: Izabela Niedziałek-Bujak
Protokolant: Rafał Komoń

po rozpoznaniu na rozprawie w dniu 16 września 2024 r. w Warszawie odwołania wniesionego do Prezesa Krajowej Izby Odwoławczej w dniu 26 sierpnia 2024 r. przez Odwołującego – Wykonawcę Prosystem Spółka Akcyjna, ul. Zygmunta Wróblewskiego 12, 51-627 Wrocław, w postępowaniu prowadzonym przez Zamawiającego – Centrum Informatyki Resortu Finansów, ul. Samorządowa 1, 26-601 Radom

przy udziale przystępującego po stronie Zamawiającego – Wykonawcy IT Solution Factor Spółka z ograniczoną odpowiedzialnością, al. Jerozolimskie 98, 00-807 Warszawa

orzeka:

1 Oddala odwołanie.

2 Kosztami postępowania odwoławczego obciąża Odwołującego – Prosystem S.A. z/s we Wrocławiu i zalicza w poczet kosztów postępowania odwoławczego kwotę 15.000 zł 00 gr. (słownie: piętnaście tysięcy złotych, zero groszy) uiszczoną przez Odwołującego tytułem wpisu od odwołania.

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

Przewodnicząca: ……

Sygn. akt: KIO 3098/24

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

W postępowaniu prowadzonym przez Zamawiającego – Centrum Informatyki Resortu Finansów z siedzibą w Radomiu, w trybie podstawowym na dostawę oprogramowania antywirusowego dla DataCenter (nr postępowania: PN/4/24/HYDB), ogłoszonym w Dzienniku Urzędowym Unii Europejskiej w dniu 08.04.2024 r., S 69/2024 204407, wobec czynności oceny ofert, wyboru oferty najkorzystniejszej, wniesione zostało w dniu 26.08.2024 r. do Prezesa Krajowej Izby Odwoławczej odwołanie Wykonawcy Prosystem S.A. z siedzibą we Wrocławiu (sygn. akt KIO 3098/24).

Odwołujący zarzucał Zamawiającemu naruszenie

1) naruszenie art. art. 91 ust. 1 w zw. z oraz art. 226 ust. 1 pkt 5 oraz art. 223 ust. 1 ustawy Pzp – poprzez:

• zaniechanie wezwania do wyjaśnień treści oferty złożonej przez Wykonawcę IT Solution Factor sp. z o.o. z siedzibą w Warszawie (dalej „IT Solution"), mimo iż oferta nie spełnia wymagań stawianych przez Zamawiającego;

• zaniechanie odrzucenia oferty złożonej przez IT Solution, mimo iż nie jest ofertą, która spełniałaby wszystkie wymagania określone w SWZ i dokumentacji postępowania;

• wybór i uznanie za najkorzystniejszą ofertę złożoną przez IT Solution, mimo iż powinna ona zostać odrzucona jako oferta, która nie spełnia wymagań określonych w SWZ i dokumentacji postępowania;

2) naruszenie art. art. 91 ust. 1 ustawy w zw. z oraz art. 226 ust. 1 pkt 5 oraz art. 223 ust.

1 ustawy Pzp – poprzez:

• zaniechanie wezwania do złożenia wyjaśnień treści oferty złożonej przez Wykonawcę Trafford IT sp. z o. o., sp. k. z siedzibą w Warszawie (dalej „Trafford IT"), mimo iż, oferta nie spełnia wymagań stawianych przez Zamawiającego;

• zaniechanie odrzucenia oferty złożonej przez Trafford IT, mimo iż nie jest ofertą, która spełniałaby wszystkie wymagania określone w SWZ i dokumentacji postępowania;

• przyznanie punktów ofercie złożonej przez Trafford IT, mimo iż powinna ona zostać odrzucona jako oferta, która nie spełnia wszystkich wymagań określonych w SWZ i dokumentacji postępowania;

3) naruszenie art. 16 ustawy Pzp – poprzez prowadzenie postępowania w sposób sprzeczny z zasadami uczciwej konkurencji i równego traktowania wykonawców.

Odwołujący wnosił o uwzględnienie odwołania w całości, nakazanie unieważnienia czynności wyboru oferty najkorzystniejszej oraz nakazanie odrzucenia ofert złożonych przez IT Solution oraz Trafford IT, a także nakazanie dokonania ponownego wyboru oferty najkorzystniejszej, tj. oferty Odwołującego.

W przypadku natomiast gdyby Izba stwierdziła konieczność uprzedniego wezwania wykonawców Trafford IT oraz IT Solution do wyjaśnień treści złożonych ofert Odwołujący wnosił o nakazanie dokonania unieważnienia czynności wyboru oferty najkorzystniejszej oraz o nakazanie wezwania wykonawców IT Solution oraz Trafford IT do złożenia wyjaśnień w zakresie złożonych ofert, a następnie nakazanie uznania, że ich oferty podlegają odrzuceniu, gdyż nie spełniają wymogów stawianych przez Zamawiającego w dokumentach postępowania.

I. Zarzuty dotyczące oferty złożonej przez IT Solution

Zdaniem Odwołującego zaoferowane oprogramowanie Trend Vision One - Endpoint Security (Essentials) producent Trend Micro, nie spełnia wymagań określonych przez Zamawiającego w OPZ.

Produkt „Trend Vision One - Endpoint Security (Essentials)“ to pakiet zawierający dwa produkty do ochrony endpoint: Standard Endpoint Protection – ochrona desktopów: Windows, macOS oraz Server and Workload Protection – ochrona serwerów: Windows, Linux. Oba produkty posiadają osobne agenty, konsole zarządzające, polityki i funkcjonalności.

Część wymagań OPZ jest spełniona tylko przez jeden z tych produktów, np. wsparcie dla systemów Linux jest jedynie w produkcie Server and Workload Protection, a wymaganie z Funkcjonalność F1 będący kryterium oceny („możliwość przywracania zaszyfrowanych plików po ataku Ransomware dla systemów Windows”) spełniany jest tylko przez produkt Standard Endpoint Protection. W takim wypadku rozwiązanie nie powinno zostać uznane za spełniające wymagania SWZ, ponieważ są to dwa osobne produkty, z osobnymi politykami i zarządzaniem. Jedynie produkt XDR (w OPZ jak EDR) czyli wykrywania zagrożeń na podstawie zgromadzonych logów i telemetrii, obejmuje wszystkie stacje.

Wymagania w OPZ odnośnie EDR to tylko 9 punktów, tj. Rozdział II, punkty od 3.1 do 3.9. Pozostałe punkty dotyczą ochrony antymalware i zarządzania stacjami końcowymi i nie jest możliwe obsłużenie pojedynczej stacji końcowej przez oba produkty, ponieważ musi zostać wybrany jeden z nich.

Dodatkowo Zamawiający w OPZ, Rozdział II, punkt 5.1 wymaga pojedynczego agenta.

Natomiast panel Trend Vision One przedstawia osobne konsole zarządzania „Standard Endpoint Protection” i „Server and Workload Protection” umieszczone w sekcji „Endpoint Security”.

Dodatkowo wymaganie Zamawiającego wyraźnie określa w OPZ, Rozdział II, punkt 7 pkt 12 „Wymagania w zakresie konsoli Centralne Zarządzanie“, że centralne zarządzanie dotyczy m.in. „dodawania własnych wpisów w ramach modułów kontroli sieci oraz kontroli urządzeń (punkt 7.10) czy „filtrowania stacji końcowych na których został zainstalowanych agent“ Posiadając agenty w dwóch różnych rozwiązaniach nie jest możliwe spełnienie wymaganych przez Zamawiającego zapisów.

Oferowane rozwiązania Trend Micro nie spełniają opisu dodatkowych funkcjonalności zapisanych w „Tom_I_SWZ_Instrukcja_dla_Wykonawcy_08-04-2024_10.16.29”, i

zaznaczonych przez Oferenta jako spełnione: a) w zakresie „Funkcjonalność F1” „Funkcjonalność F1

Oprogramowanie zapewnia możliwość przywracania zaszyfrowanych plików po ataku Ransomware dla systemów Windows“

Trend Micro łączy funkcjonalności dwóch różnych produktów „Standard Endpoint Protection” i „Server and Workload Protection” w paczce Trend Vision One Essentials. Przywracanie zaszyfrowanych plików jest możliwe w produkcie Standard Endpoint Protection, który m.in. nie obsługuje systemów Linux i ma zupełnie inne funkcjonalności niż produkt Server and Workload Protection, który obsługuje systemy Linux.

Do obu tych produktów jest osobny agent i oddzielne zarządzanie. W konsoli TM jest wyraźne rozróżnienie na „Standard Endpoint Protection Manager” i „Server and Workload Protection Manager”. W celu zapewnienia odzyskiwania plików trzeba umieścić stacje w osobnym, dedykowanym dla desktopów produkcie „Standard Endpoint Protection Manager” i zarządzać nimi z tego miejsca. Polityki, grupy, ustawienia, notyfikacje itd. są zupełnie inne i nie synchronizują się pomiędzy produktami.

Możliwość przywracania zaszyfrowanych plików po ataku Ransomware jest dostępna tylko w produkcie „Standard Endpoint Protection Manager”. Zgodnie z OPZ rozwiązanie ma wspierać systemy Windows i Linux, np. Rozdział II, punkt 5.6. „możliwość automatycznej aktualizacji agentów zainstalowanych na stacjach końcowych z systemem operacyjnym: Microsoft Windows oraz Linux;”. Oferta zawierająca rozwiązanie Trend Micro nie spełnia jednocześnie wszystkich punktów OPZ.

W OPZ jest położony duży nacisk na Centralną Konsolę Zarządzania i jej funkcjonalności (OPZ, Rozdział II, punkt „7. Wymagania w zakresie konsoli Centralne Zarządzanie:”). A zatem nie jest możliwe dopuszczenie rozwiązania, które część funkcjonalności spełnia w jednej konsoli zarządzającej a część w drugiej. Zarządzając

systemami Windows w konsoli „Standard Endpoint Protection Manager", żeby spełnić Funkcjonalność F1, oraz systemami Linux w konsoli „Server and Workload Protection Manager" (bo tylko ta konsola może zarządzać Linuxami) nie spełnione są punkty centralnego zarządzania zawarte w OPZ takie jak 7.8, 7.10, 7.14, 7.15, 7.16, 7.17, 7.19. Samo słowo „manager", tj. menadżer w nazwach „Standard Endpoint Protection Manager" i „Server and Workload Protection Manager" wskazuje na oddzielne zarządzanie. Posiadanie części stacji w jednej a części w drugiej konsoli zarządzającej powoduje, że nie są spełnione punkty OPZ „6. Zarządzanie Politykami Bezpieczeństwa musi uwzględnić:". Opisują one tworzenie polityk czy list kontroli sieci. Nie można stworzyć polityki czy listy kontroli sieci obejmującej system Windows i Linux oraz spełniającej Funkcjonalność F1. Z kolei wymagane są wszystkie z tych trzech zapisów (Funkcjonalność F1 jest wymagana, ponieważ Oferent wskazał ją jako spełnioną).

b) w zakresie Tomu III SWZ

Oferowane rozwiązanie TM nie spełnia wymagań „Tom_III_SWZ_-_Opis_przedmiotu_zamowienia_wersja_ujednolicona_13-052024_09.31.29.pdf" 1. Rozdział II OPZ, punkt 4.3

„Automatyczna Reakcja i Izolacja Zagrożeń musi posiadać: „zestaw silników które można włączać lub wyłączać;"

W rozwiązaniu nie można wyłączyć silników jako automatyczna reakcja ani podczas izolacji zagrożeń. Wszystkie możliwe czynności dla automatycznej reakcji i izolacji zagrożeń Odwołujący przedstawił na zrzucie ekranu z oferowanych rozwiązań Tren Micro. Nie ma tu możliwości wyłączania lub włączania zestawu silników czego wymaga Zamawiający.

2. Rozdział II OPZ, punkt 4.5

„możliwość przeniesienia do kwarantanny złośliwych plików należących do tego samego incydentu. Funkcja kwarantanny musi zatrzymać procesy, szyfrować plik wykonywalny i przenieść go na ograniczoną ścieżkę;"

Oferowane rozwiązania Trend Micro nie zawierają opcji przeniesienia wszystkich plików z incydentu do kwarantanny. Pliki w incydencie można dodać do listy blokowania, co nie jest jednoznaczne z kwarantanną, dodawać pliki można tylko pojedynczo. Odwołujący przedstawił zrzut z ekranu z konsoli Trend Micro, gdzie widoczna jest możliwość dodania pliku do listy blokowania.

W dostępnych opcjach oferowane rozwiązanie nie posiada możliwości przeniesienia do kwarantanny złośliwych plików należących do tego samego incydentu czego wymaga Zamawiający.

3. Rozdział II OPZ, punkt 5.1

„Jedno plikowy agent AV, który musi być w pełni autonomiczny, co oznacza, że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani ŻADNYCH zasobów zewnętrznych od agenta;"

Brak Internetu uniemożliwia oferowanym rozwiązaniom Trend Micro działanie funkcjonalności: behavior monitoring (tłumaczenie z ang.: monitorowanie/analiza

behawioralna), predictive machine learning (tłumaczenie z ang.: predyktywne uczenie maszynowe), i process memory scanning (tłumaczenie z ang.: skanowanie procesów w pamięci).

„If your agents or relays don't have access to the internet (also called "air-gapped agents"), then they won't be able to access several of the security services provided by the Trend Micro Smart Protection Network. These security services are necessary for the full and successful operation of the Server & Workload Protection Anti-Malware and Web Reputation features. The Trend Micro Smart Protection Network security services are:

Jeśli agenci lub przekaźniki nie mają dostępu do Internetu (zwani również „agentami ze szczeliną powietrzną"), nie będą mogli uzyskać dostępu do kilku usług zabezpieczeń świadczonych przez Trend Micro Smart Protection Network. Te usługi bezpieczeństwa są niezbędne do pełnego i pomyślnego działania funkcji Server & Workload Protection Anti-Malware i Web Reputation. Usługi bezpieczeństwa Trend Micro Smart Protection Network to: Smart Scan Service Smart Scan

Web Reputation Service Web Reputation

Global Census Service Behavior monitoring, predictive machine learning

Good File Reputation Service Behavior monitoring, predictive machine learning,

process memory scans

Predictive Machine Learning Service Predictive machine learning

„Źródło:

Z oficjalnej dokumentacji producenta Trend Micro wynika, że najważniejsze funkcjonalności, takie jak monitorowanie behawiorystyczne i uczenie maszynowe nie działają przy braku dostępu do zasobu zewnętrznego jakim jest chmura, tj. Internet a takiej pracy produktu wymaga Zamawiający.

4. Rozdział II OPZ, punkt 5.9.2

„funkcjonalność automatycznej aktualizacji, która musi pozwalać na wybór stacji końcowych które powinny zostać zaktualizowane posiadając możliwość wyboru co najmniej: jedynie stacji końcowych z wybranym tag-iem;”

Oferowane rozwiązania Trend Micro nie spełniają tego zapisu.

Standard Endpoint Protection Manager posiada tagowanie endpointów, ale nie ma możliwości definiowania aktualizacji na podstawie tagów. Server and Workload Protection

Manager ma tagi tylko dla zdarzeń/logów, nie ma dla endpointów. Odowłujący załączył zrzuty ekranu z interfejsu oferowanych rozwiązań Trend Micro. Widać na nich, że w opcjach automatycznej aktualizacji nie można wybrać stacji końcowych podlegających aktualizacji na podstawie tagu czego wymaga Zamawiający.

5. Rozdział II OPZ, punkt 5.12

„możliwość zdefiniowania maksymalnej liczby stacji końcowych pobierających jednocześnie paczkę aktualizacyjną;”

Oferowane rozwiązania Trend Micro nie spełniają tego zapisu, nie ma takiej opcji. Brak tej opcji jest widoczny na zrzutach ekranu z oferowanych rozwiązań Trend Micro. Pośród wszystkich dostępnych opcji nie ma opcji definiowania maksymalnej liczby stacji końcowych pobierających jednocześnie paczkę aktualizacyjną.

6. Rozdział II OPZ, punkt 5.18

„informacje dla każdego pakietu instalacyjnego, które muszą zawierać co najmniej następujące dane:

5.18.1 wersja główna,

5.18.2 numer buildu,

5.18.3 rozszerzenie pliku,

5.18.4 nazwa pliku,

5.18.5 data opublikowania,

5.18.6 platforma”

Informacje zawarte w punktach od 5.18.1 do 5.18.6 nie są wyświetlane w Standard Endpoint Protection Manager a w Server and Workload Protection Manager nie ma „daty opublikowania”.

W kolumnach tabeli zawierającej pakiety instalacyjne są kolumny „Nazwa”, „Platforma”, „Wersja”, „Typ publikacji” i „Data importu”. Nie istnieje kolumna „Data opublikowania” czego wymaga Zamawiający. Data importu jest myląca dla administratorów, ponieważ może być różna dla tego samego pakietu (np. przy ponownym pobraniu) i niezgodna chronologicznie w porównaniu z datą opublikowania, np. starszy pakiet instalacyjny może być zaimportowany później niż nowszy. Data opublikowania jest niezmienna i niezależna od momentu pobrania pakietu instalacyjnego.

7. Rozdział II OPZ, punkt 6.10

„możliwość stopniowania poziomu wyjątków dla wyjątków typu "Ścieżka" w systemie Windows , co najmniej w następującym zakresie:

6.10.1 wygaszenie alarmów,

6.10.2 zredukowanie monitorowania konkretnego procesu,

6.10.3 zredukowanie monitorowania konkretnego procesu i jego procesów potomnych,

6.10.4 wyłączenie monitorowania konkretnego procesu,

6.10.5 wyłączenie monitorowania konkretnego procesu i jego procesów potomnych;”

Oferowane rozwiązania Trend Micro nie spełniają tego zapisu opcji 6.10.1 do 6.10.5 dla ścieżki/path systemu Windows, co przedstawiono na zrzutach ekranu. Na zrzutach ekranu widoczne są opcje konfiguracji wyjątków typu „ścieżka” w systemie, nie ma jednak opcji przedstawionych w podpunktach 6.10.1 do 6.10.5 czyli możliwości określenia stopnia poziomu wyjątku tego typu.

Zrzuty ekranów pochodzą z konfiguracji polityki w produktach ochrony antymalware. Funkcjonalność XDR jest osobna i niezależna od produktów Standard Endpoint Protection Manager i Server and Workload Protection Manager. W konsoli oferowanych rozwiązań Trend Micro, w opcjach wykrywania zagrożeń za pomocą XDR są opcje 6.10.1, 6.10.4, 6.10.5. Podpunkt 6.10 należy do punktu „6. Zarządzanie Politykami Bezpieczeństwa musi uwzględnić:” czyli do ustawień polityk. Jeżeli w wykrywaniu zagrożeń za pomocą telemetrii XDR zostaną wprowadzone wyjątki, to nie będą one działać

podczas wykrywania zagrożeń bezpośrednio w produktach Standard Endpoint Protection Manager i Server and Workload Protection Manager czyli w rzeczywistym oprogramowaniu antywirusowym. Dlatego wyjątki możliwe do wprowadzenia w produkcie XDR nie powinny być brane pod uwagę. Jednak nawet, uwzględniając opcje wyjątków w produkcie XDR, nie są spełnione punkty 6.10.2, 6.10.3 8. Rozdział II OPZ, punkt 6.11

„rozwiązanie, dla wyjątków typu "Ścieżka" w systemie Linux musi mieć możliwość stopniowania poziomu wyjątków, co najmniej w następującym zakresie:

6.11.1 wygaszenie alarmów,

6.11.2 wyłączenie monitorowania konkretnego procesu”

Oferowane rozwiązania Trend Micro nie spełniają tego zapisu. Nie ma opcji 6.11.1 i 6.11.2 dla ścieżki/path systemu Linux co przedstawiono na zrzutach ekranu

Zrzuty ekranów pochodzą z konfiguracji polityki w produktach ochrony antymalware. Funkcjonalność XDR jest osobna i niezależna od produktów Standard Endpoint Protection Manager i Server and Workload Protection Manager. Opcje opisane w punktach 6.11.1 i 6.11.2 są tylko dostępne w wyjątkach wykrywania zagrożeń za pomocą XDR, nie dla antywirusa/polityki agenta. Podpunkt 6.10 należy do punktu „6. Zarządzanie Politykami Bezpieczeństwa musi uwzględnić:” czyli do ustawień polityk a w ustawieniach polityki nie ma opisanych opcji. Jeżeli w wykrywaniu zagrożeń za pomocą telemetrii XDR zostaną wprowadzone wyjątki, to nie będą one działać podczas wykrywania zagrożeń bezpośrednio w produktach Standard Endpoint Protection Manager i Server and Workload Protection Manager czyli w rzeczywistym oprogramowaniu antywirusowym. Dlatego wyjątki możliwe do wprowadzenia w produkcie XDR nie powinny być brane pod uwagę.

9. Rozdział II OPZ, punkt 6.18

„moduł kontroli sieci, który musi być zintegrowany z funkcjonalnością tagowania hostów w oferowanym rozwiązaniu”

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania. Standard Endpoint Protection Manager posiada tagowanie endpointów ale nie można ich wykorzystać w module kontroli sieci. Server and Workload Protection Manager posiada tagi tylko dla zdarzeń/logów, nie ma tagowania dla endpointów. Nie ma integracji modułu kontroli sieci z tagowaniem hostów. Możliwość tagowania ograniczająca się tylko do zdarzeń/logów w produkcie Server and Workload Protection Manager przedstawiono na h zrzutach ekranu.

Tylko dla zdarzeń, które na zrzucie są widoczne jako kolejne rzędy, można dodać tag („Add Tag(s)”).

10. Rozdział II OPZ, punkt 6.20

„interfejs graficzny modułu kontroli sieci, który musi oferować możliwość importowania wybranych wyjątków dla kwarantanny sieciowej rozwiązania z pliku .json.”

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania. Rozwiązania Trend Micro potrafią jedynie zaimportować plik z formatu XML co przedstawiają zrzuty ekranu z konsoli Trend Micro. Pokazują one możliwość eksportu reguł, w tym wyjątków czyli reguł dopuszczających ruch, do formatu możliwego do zaimportowania w postaci XML, tj. „Export to XML (For Import)” czyli „Eksport do formatu XML (na potrzeby importu)” oraz „Export Selected to XML (For Import)” czyli „Eksport wybranych reguł do formatu XML (na potrzeby importu)”.

Zrzut przedstawia przykład importowania reguł, w tym wyjątków czyli reguł dopuszczających ruch. Jedyna opcja dostępna do importu to „Import From File” czyli „Import z pliku”.

Po wyborze opcji „Import z pliku” pojawia się okno polecające wybór pliku XML do importu, tj. „Please select an XML file of firewall rules to import” czyli „Proszę wybrać plik XML reguł zapory sieciowej do importu”.

XML to odmienny format pliku niż JSON. Posiada inną strukturę wewnętrzną. JSON (JavaScript Object Notation) to otwarty standardowy format tekstowy do wymiany danych. Podczas przetwarzania informacji JSON wykorzystuje mniej pamięci niż XML co powoduje, że JSON jest lepszym formatem do szybkiego przetwarzania dużych ilości danych. Nie jest możliwe zastosowanie tego samego analizatora składniowego (parsera) do obu formatów jednocześnie co sprawia, że formaty JSON i XML nie są zamienne.

11. Rozdział II OPZ, punkt 7.12

„7.12 rozwiązanie musi mieć możliwość filtrowania stacji końcowych na których został zainstalowanych agent, co najmniej z wykorzystaniem następujących parametrów:

7.12.1 nazwa stacji końcowej,

7.12.2 tag przypisany do stacji końcowej,

7.12.3 system operacyjny stacji końcowej,

7.12.4 wersja zainstalowanego agenta,

7.12.5 typ stacji końcowej:

7.12.5.1 desktop,

7.12.5.2 serwer,

7.12.6 domena MS Windows,

7.12.7 czy agent połączony jest do konsoli zarządzania,

7.12.8 stan zdrowia agenta,

7.12.9 stan sieci stacji końcowej,

7.12.10 czy było wykonane pełne skanowanie dysku,

7.12.11 czy agent oczekuje na aktualizacje,

7.12.12 architekturę systemu operacyjnego,

7.12.13 rodzaj użytego instalatora,

7.12.14 stan operacyjny,

7.12.15 jakikolwiek ciąg znaków z domeny Microsoft Windows,

7.12.16 MAC adres.,

7.12.17 lokalny adres IP."

Rozwiązania Trend Micro nie spełniają punktów 7.12.2, 7.12.6, 7.12.9, 7.12.15.

Zrzuty ekranu pochodzą z różnych konsol zarządzania, punkty, które nie są spełnione dotyczą wszystkich konsol.

W każdej z konsol jest tylko część wymienionych parametrów. Zarządzanie produktem w takim stanie jest niedopuszczalne i niezgodne ze zwrotem „konsoli centralnego Zarządzania" użytym w OPZ. Dodatkowo dwie konsole należą do produktu Standard Endpoint Protection Manager, który nie obsługuje systemów Linux. Prowadzi to do sytuacji, w której Zamawiający będzie musiał prowadzić ewidencję, które informacje są przechowywane w której konsoli oraz nie będzie posiadał dostępu do informacji o wszystkich stacji końcowych, ponieważ stacje mogą być umieszczone w różnych produktach i w konsoli z daną informacją nie będzie części agentów. Przy skali zamawianego oprogramowania, tj. 8500 szt. endpointów spowoduje to ogromny chaos w zarządzaniu i ograniczenie funkcjonalności.

Zrzuty przedstawiają wszystkie możliwe opcje filtrowania stacji końcowych. Nie istnieje możliwość filtrowania po wymaganych parametrach, tj. 7.12.2 tag przypisany do stacji końcowej, 7.12.6 domena MS Windows, 7.12.9 stan sieci stacji końcowej, 7.12.15 jakikolwiek ciąg znaków z domeny Microsoft Windows a takich funkcjonalności wymaga Zamawiający.

12. Rozdział II OPZ, punkt 7.15, 7.16, 7.19

„7.15 rozwiązanie musi umożliwiać oznaczanie hostów poprzez etykiety (tagi);

7.16 każda etykieta (tag) musi być określana poprzez parametr - nazwa etykiety (tagu);

7.19 rozwiązanie musi umożliwiać dopisanie wielu etykiet (tagów) do jednej stacji końcowej;" Standard Endpoint Protection Manager posiada tagowanie endpointów ale nie obsługuje serwerów Linux, które są wymagane do obsługi zgodnie z wymaganiami OPZ, np. Rozdział II, punkt 5.6. „możliwość automatycznej aktualizacji agentów zainstalowanych na stacjach końcowych z systemem operacyjnym: Microsoft Windows oraz Linux;". Server and Workload Protection Manager posiada tagi tylko dla zdarzeń/logów, nie posiada tagów dla hostów/stacji końcowych. Możliwość tagowania ograniczająca się tylko do zdarzeń/logów w produkcie Server and Workload Protection Manager przedstawiona została na zrzutach ekranu z konsoli rozwiązań Trend Micro.

Tylko dla zdarzeń, które na powyższym zrzucie ekranu są widoczne jako kolejne rzędy, można dodać tag („Add Tag(s)").

13. Rozdział II OPZ, punkt 7.17

„7.17 etykiety (tagi) muszą umożliwiać filtrowanie stacji końcowych, tworzenia grup dynamicznych oraz do tworzenie widżetów na pulpicie nawigacyjnym;"

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania.

Server and Workload Protection Manager posiada tagi tylko dla zdarzeń/logów, nie posiada tagów dla hostów/stacji końcowych. Produkt nieobsługujący systemów Linux, Standard Endpoint Protection Manager, nie posiada takiej

funkcjonalności.

Możliwości produktu Standard Endpoint Protection Manager odnośnie tagów ograniczają się do przeszukiwania logów i tworzenia raportów dla endpointów z określonym tagiem. Możliwości odnośnie tagowania zostały na wycinku z dokumentacji producenta Trend Micro.

Wycinek z dokumentacji Trend Micro: (tłumaczenie z ang.):

- Widok danych zapytania dziennika Dostępu Użytkownika zawiera szczegółowe

informacje o wszelkich modyfikacjach użytkownika związanych z dowolnymi dostępnymi niestandardowymi tagami lub filtrami. Aby uzyskać więcej informacji, zapoznaj się z następującymi tematami: o Zapytania dotyczące dzienników

- Generowanie niestandardowych raportów dla oznaczonych użytkowników i punktów

końcowych, na podstawie skojarzonych tagów, filtrów lub etykiety ważności jako cele raportu. Aby uzyskać więcej informacji, zapoznaj się z następującymi tematami:

o Tworzenie raportów jednorazowych

o Dodawanie zaplanowanych raportów

o Edytowanie zaplanowanych raportów)

Odnośnik do dokumentacji Trend Micro:

us/documentation/article/trend-vision-one-custom-tags-filters

14. Rozdział II OPZ, punkt 8.9

„8.9 interfejs graficzny modułu kontroli sieci, który musi prezentować reguły w formie tabularycznej, z możliwością definiowania następujących kolumn:

8.9.1 nazwa,

8.9.2 opis,

8.9.3 aplikacja,

8.9.4 poziomami struktury rozwiązania, dla których reguły są aplikowane,

8.9.5 system operacyjny,

8.9.6 status (włączona / wyłączona),”

Oferowane rozwiązania Trend Micro nie spełniają punktów 8.9.3 do 8.9.6, co zostało zaprezentowane na zrzutach ekranu z konsoli.

Zrzuty ekranu przedstawiają wszystkie możliwe do zdefiniowania kolumny prezentowanych reguł w formie tabelarycznej interfejsu graficznego modułu kontroli sieci. Oferowany produkt nie posiada możliwości definiowania kolumn wyszczególnionych w punktach 8.9.3 do 8.9.6.

15. Rozdział II OPZ, punkt 9.4

„zakres czasu raportów, który musi być możliwy do zdefiniowania przez użytkownika konsoli zarządzającej;”

W oferowanych rozwiązaniach Trend Micro użytkownik nie może zdefiniować zakresu, może tylko wybrać zakres z listy zdefiniowanej przez producenta, w przypadku raportów z harmonogramu (Scheduled report), jest to lista zdefiniowanej przez producenta z opcjami dzień, tydzień, miesiąc, w przypadku jednorazowych raportów (One time report), jest to lista z opcjami 7 dni, 30 dni. Przedstawiono zrzuty, które opisują konfiguracje, w których brakuje możliwości zdefiniowania zakresu.

Podczas prazy z innymi funkcjonalnościami istnieje możliwość definiowania zakresu czasu, np. dla wyszukiwania zdarzeń w funkcjonalności XDR. Przedstawiono na zrzucie ekranu możliwość wyboru definiowanego zakresu (Custom period) w wyszukiwaniu zdarzeń XDR. Można wybrać dzień i godzinę, od której („From:”) oraz do której („To:”) wyszukiwanie będzie obowiązywać. Podczas tworzenia raportów rozwiązanie nie daje takiej możliwości więc nie spełnia cytowanego wymagania, którego spełnienia wymaga Zamawiający.

16. Rozdział II OPZ, punkt 10.14

„10.14 moduł zarządzania aktywnościami, który musi oferować możliwość filtrowania logów w następujących kategoriach:

10.14.1 odpowiedź na zagrożenia;

10.14.2 zarządzanie incydentami;

10.14.3 wykluczenia;

10.14.4 operacje administratorskie;

10.14.5 email użytkownika konsoli;

10.14.6 nazwa hosta.”

Oferowane rozwiązania Trend Micro nie spełniają tego zapisu.

Rozwiązanie nie posiada filtrowania logów w kategoriach 10.14.1, 10.14.2, 10.14.3, 10.14.5, co przedstawiono na zrzutach ekranu z konsoli oferowanych rozwiązań Trend Micro.

Przedstawione są wszystkie możliwe do filtrowania kategorie. Oferowane rozwiązania nie posiadają filtrowania logów w kategoriach 10.14.1, 10.14.2, 10.14.3, 10.14.5.

17. Rozdział II OPZ, punkt 10.15

„moduł zarządzania aktywnościami, który musi oferować możliwość eksportowania wpisów 100, 1000, 5000 lub 10000 ostatnich aktywności do pliku .csv.”

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania.

Dla modułu zarządzania aktywnościami nie ma możliwości eksportu określonej liczby wpisów, czego wymaga Zamawiający i co jest przedstawione na zrzutach ekranu z konsoli oferowanych rozwiązań Trend Micro.

Po wybraniu opcji „Export as .csv file.” czyli „Eksportuj jako plik .csv” eksportowane są wszystkie wyświetlone wpisy.

18. Rozdział II OPZ, punkt 10.16

„moduł zarządzania aktywnościami, który musi oferować możliwość pobierania logów zebranych przez agenta końcowego po wydaniu komendy z poziomu modułu zarządzania;”

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania.

Moduł zarządzania aktywnościami (Audit Log) nie ma takiej opcji, co potwierdza poniższy zrzut ekranu z konsoli oferowanych rozwiązań Trend Micro a czego wymaga Zamawiający.

Na zrzucie ekranu z modułu zarządzania aktywnościami (Audit Log) jedynymi dostępnymi opcjami jest filtrowanie wpisów i eksportowania ich jako pliku CSV.

19. Rozdział II OPZ, punkt 10.23

„zarządzanie notyfikacjami, które musi umożliwiać wyszukiwanie pojedynczego rodzaju zdarzenia poprzez wyszukiwarkę tekstową;”

Oferowane rozwiązania Trend Micro nie spełniają tego wygania, nie posiada wyszukiwania powiadomień, co zaprezentowano na zrzuci ekranu z konsoli oferowanych rozwiązań Trend Micro.

Na zrzucie ekranu nie ma okna lub sekcji, w której można przeprowadzić wyszukiwanie powiadomień. Jest dostępna lista powiadomień ale nie można ich wyszukać poprzez wyszukiwarkę tekstową.

20. Rozdział II OPZ, punkt 10.24

6. „10.24 zarządzanie notyfikacjami, które musi wyróżniać następujące typy powiadomień:

10.24.1 administracyjne;

10.24.2 kontrola urządzeń;

10.24.3 tagi urządzeń;

10.24.4 kontrola firewall;

10.24.5 malware;

10.24.6 łagodzenie incydentów;

10.24.7 operacje;

10.24.8 Remote Shell;”

Oferowane rozwiązania Trend Micro nie spełniają podpunktów 10.24.3, 10.24.6 oraz 10.24.8, co przedstawiono na zrzucie ekranów z konsoli oferowanych rozwiązań Trend Micro.

Zrzuty ekranów przedstawiają miejsca, w których można konfigurować notyfikacje. Ponieważ oferta składa się z wielu produktów, konfiguracja notyfikacji nie jest możliwa w pojedynczym panelu. Na zrzutach ekranów przedstawiono wszystkie możliwe do skonfigurowania notyfikacje. Oferowane rozwiązania Trend Micro nie wyróżniają typów powiadomień opisanych w podpunktach 10.24.3, 10.24.6 oraz 10.24.8 czego wymaga

Zamawiający.

II. Zarzuty dotyczące oferty złożonej przez Trafford IT

Zgodnie ze złożoną ofertą, Trafford IT, zaoferowało oprogramowanie Cortex XDR producent Palo Alto Networks.

W ocenie Odwołującego zaoferowane oprogramowanie nie spełnia wymagań określonych przez Zamawiającego w opisie przedmiotu zamówienia. W ofercie nie podano rodzaju licencji, co uniemożliwia wskazanie konkretnego rozwiązania. W ofercie wymieniony jest produkt „Cortex XDR” ale ten produkt nie jest sprzedawany w takiej formie, jest sprzedawany jako Cortex XDR Prevent lub Cortex XDR Pro. W formularzu ofertowym wyraźnie napisano: „należy podać oznaczenie pozwalające na identyfikację oprogramowania oraz rodzaju licencji” Wpisanie „Cortex XDR” nie spełnia tego wymagania.

W opisie produktu na stronie Palo Alto - -

Producent wskazuje: „Two powerful offerings.” (tłumaczenie z ang.: „Dwie potężne oferty.”) „CORTEX XDR PREVENT - CORTEX XDR PRO” Tylko powyższe opcje są właściwe. Są to różne produkty, do każdego z tych dwóch rodzajów licencji jest osobna instrukcja, tzw. admin guide. Licencje te różnią się znacznie funkcjonalnością. Cortex Pro pozwala na szerszy zakres ochrony i funkcjonalności. Ze złożonej oferty Zamawiający nie jest w stanie zidentyfikować jaki produkt otrzyma.

Jeżeli nawet by przyjąć (mimo iż nie wynika to z treści złożonej oferty), że zaoferowano produkt „Cortex XDR Pro“, to Odowłujący wskazał funkcjonalności, których ten produkt nie posiada w odniesieniu do dokumentu: „Tom_III_SWZ_

_Opis_przedmiotu_zamowienia_wersja_ujednolicona_13-05-2024_09.31.29.pdf”.

1. Rozdział II OPZ , punkt 5.18

„informacje dla każdego pakietu instalacyjnego, które muszą zawierać co najmniej następujące dane:

5.18.1 wersja główna,

5.18.2 numer buildu,

5.18.3 rozszerzenie pliku,

5.18.4 nazwa pliku,

5.18.5 data opublikowania,

5.18.6 platforma”

Oferowane rozwiązanie nie posiada 5.18.3, 5.18.4, co zaprezentowano na zrzucie ekranu z konsoli oferowanego produktu Palo Alto.

2. Rozdział II OPZ, punkt 6.8.1

„6.8 możliwość tworzenia wyjątków dla systemu Microsoft Windows z wykorzystaniem następujących elementów:

6.8.1 HASH SHA1,

6.8.2 ścieżka do pliku,

6.8.3 ścieżka do katalogu wraz z katalogami podrzędnymi,

6.8.4 certyfikat,

6.8.5 rodzaj pliku”

Oferowane rozwiązanie nie spełnia punktu 6.8.1. Wspierany jest tylko SHA256. Odwołujący przedstawił wycinek z dokumentacji producenta Palo Alto oraz odnośnik do strony dokumentacji potwierdzający ten fakt.

Wycinek dokumentacji: (tłumaczenie z ang.):

1. Przejdź do Incident Response → Response → Action Center → + New Action.
2. Wybierz opcję Add to Block List lub Add to Allow List.
3. Wprowadź skrót SHA-256 pliku i kliknij

Możesz dodać maksymalnie 100 skrótów plików na raz. Możesz dodać komentarz, który zostanie dodany do wszystkich skrótów dodanych w tej akcji.)

Strona do dokumentacji technicznej oferowanego produktu Palo Alto:

3. Rozdział II OPZ, punkt 6.12 „gotowy katalog wyjątków przygotowany dla wybranych

aplikacji i aktualizowany przez producenta;”

Nie ma przygotowanego katalogu wyjątków dla wybranych aplikacji. Jest tylko przygotowana lista aplikacji do blokowania, co w tym wypadku jest odwrotną funkcjonalnością. Według odnośnika do strony dokumentacji technicznej https://docs-

cortex.paloaltonetworks.com/r/Cortex-XDR/Cortex-XDR-Pro-AdministratorGuide/Add-a-New-Malware-Security-Profile producenta Palo Alto (tłumaczenie z ang.:

Predefiniowane zablokowane aplikacje Lista aplikacji Lista powszechnie znanych

aplikacji, które Twoja organizacja może chcieć zablokować na nadzorowanych urządzeniach, znajduje się tutaj. Agent Cortex XDR zablokuje korzystanie z wybranych aplikacji. Możesz wybrać jedną lub więcej aplikacji.

Odwołujący przedstawił także zrzuty ekranu z oferowanego rozwiązania Palo Alto potwierdzające brak gotowego katalogu wyjątków dla wybranych aplikacji.

4. Rozdział II OPZ, punkt 6.15 „możliwość konfigurowania list blokujących na różnych

poziomach hierarchii z zachowaniem zasad dziedziczenia z wyższych poziomów do niższych;”

Oferowane rozwiązanie producenta Palo Alto nie posiada dziedziczenia z wyższych poziomów hierarchii do niższych, nie ma więc możliwości dziedziczenia list blokujących w takiej hierarchii.

5. Rozdział II OPZ, punkt 8.9.4

„8.9 interfejs graficzny modułu kontroli sieci, który musi prezentować reguły w formie tabularycznej, z możliwością definiowania następujących kolumn:

8.9.1 nazwa,

8.9.2 opis,

8.9.3 aplikacja,

8.9.4 poziomami struktury rozwiązania, dla których reguły są aplikowane,

8.9.5 system operacyjny,

8.9.6 status (włączona / wyłączona),

8.9.7 akcja (zezwalaj / blokuj),

8.9.8 kierunek transmisji,

8.9.9 lokalny host,

8.9.10 lokalny port,

8.9.11 zdalny host,

8.9.12 zdalny port,”

Rozwiązanie nie spełnia punktu 8.9.4. Listę dostępnych kolumn zaprezentowano na zrzucie ekranu z konsoli oferowanego rozwiązania Palo Alto.

6. Rozdział II OPZ, punkt 8.14 „8.14 moduł kontroli sieci z włączonym firewall nie może

być zarejestrowany jako firewall w systemie Linux. Firewall rozwiązania musi działać równolegle do firewalla systemowego systemu Linux. W przypadku konfliktu między

firewallami systemowym a rozwiązania, zasady firewalla rozwiązania muszą traktowane być priorytetowo;”

Oferowane rozwiązanie nie posiada firewall dla systemu Linux, co potwierdza wyciąg z dokumentacji technicznej oraz odnośnik do strony dokumentacji technicznej producenta Palo Alto

Wycinek z dokumentacji technicznej Palo Alto (tłumaczenie z ang.):

Zapora hosta

Zapora hosta Cortex XDR umożliwia kontrolowanie komunikacji na punktach końcowych. Aby użyć zapory hosta, należy ustawić reguły, które zezwalają na ruch na urządzeniach lub go blokują, i zastosować je do punktów końcowych za pomocą reguł zasad zapory hosta. Ponadto można skonfigurować różne zestawy reguł w oparciu o bieżącą lokalizację punktów końcowych — w obrębie lub poza siecią organizacji. Reguły zapory hosta Cortex XDR wykorzystują interfejsy API zapory systemu operacyjnego i wymuszają te reguły na punktach końcowych, ale nie na ustawieniach zapory systemu Windows lub Mac.

Odwołujący wymienił reguły dotyczące zasad zapory hosta Cortex XDR na punktach końcowych dla platform Windows i Mac, Linux – nieobsługiwana.

Strona do dokumentacji technicznej oferowanego produktu Palo Alto: .

W ocenie Odwołującego obie złożone oferty są niezgodne z SWZ i załącznikami do niej (stanowiącymi dokumentację postępowania). Oferty obu tych Wykonawców powinny zostać odrzucone, jako niezgodne z SWZ.

Zamawiający złożył odpowiedź na odwołanie wnosząc o jego oddalenie w całości (pismo z 12.09.2024 r.)

Przystępujący po stronie Zamawiającego – IT Solution Factor Sp. z o.o. złożył pismo procesowe, w którym odniósł się do zarzutów skierowanych wobec jego oferty (pismo z 12.09.2024 r.).

Odwołujący na posiedzeniu przed otwarciem rozprawy wycofał zarzut dotyczący oferty IT Solution Factor Sp. z o.o. i jej niezgodności z opisanym w lit a wymaganiem „Funkcjonalność F1”. Jednocześnie Odwołujący podtrzymał zarzut, iż zaoferowany produkt: „Trend Vision One - Endpoint Security (Essentials)“, to pakiet zawierający dwa produkty do ochrony endpoint: Standard Endpoint Protection – ochrona desktopów: Windows, macOS oraz Server and Workload Protection – ochrona serwerów: Windows, Linux. Oba produkty posiadają

osobne agenty, konsole zarządzające, polityki i funkcjonalności, co ma naruszać wymagania z rozdziału II OPZ.

W pozostałym zakresie Odwołujący podtrzymał odwołanie, kwestionując prawidłowość dwóch ofert, tj. wykonawców IT Solution Factor Sp. z o.o. oraz Trafford IT.

Izba oddaliła odwołanie w całości uznając, iż okoliczności wskazane w podstawie zarzutów nie uzasadniały uznania, iż obie kwestionowane oferty podlegać winny odrzuceniu, jako niezgodne z warunkami zamówienia, jak również nie uzasadniały twierdzenia o potrzebie wyjaśnienia treści ofert.

Odwołanie w zasadniczym zakresie sprowadzało się do wykazania niezgodności obu ofert z swz, mającej uzasadniać ich odrzucenie na podstawie art. 226 ust. 1 pkt 5 Ustawy. Kwestia wyjaśnienia treści ofert, poza jej wskazaniem w zarzutach naruszenia Ustawy nie została w żaden sposób rozwinięta w uzasadnieniu i sprowadzała się do ogólnego stwierdzenia zaniechania przez Zamawiającego wezwania obu wykonawców do wyjaśnienia treści oferty pomimo niespełniania wymagań Zamawiającego. W tych okolicznościach zarzut dotyczący zaniechania wezwania do złożenia wyjaśnień nie mógł być uwzględniony i przy braku jakiejkolwiek rozwinięcia w uzasadnieniu, jego oddalenie również można sprowadzić do stwierdzenia o lakoniczności odwołania, lub wręcz braku prawidłowo podniesionego zarzutu. Odwołujący w żadnym miejscu obszernego uzasadnienia nie wskazał w jakim zakresie treść oferty mogła podlegać wyjaśnieniu przy jednoczesnym żądaniu odrzucenia obu ofert, jako niezgodnych z warunkami zamówienia. Powyższe czyniło niejasnym ustalenie, czego miałyby dotyczyć wyjaśnienia, a tym samym uniemożliwiało to merytoryczną ocenę zarzutu.

Odnosząc się natomiast do pozostałych zarzutów odwołania, należy tytułem wstępu poczynić ogólna uwagę, iż konstrukcja zarzutów ograniczała ich rozpoznanie wyłącznie do zakresu okoliczności wskazanych w uzasadnieniu zarzutów. Izba pominęła argumentację podnoszoną przez Odwołującego w odpowiedzi na stanowiska pisemne Zamawiającego i Przystępującego po jego stronie, która wykraczała poza kwestie faktyczne wskazane w odwołaniu. Odwołujący formułował zarzuty niezgodności treści oferty z swz, wskazując i cytując konkretne postanowienie opisujące warunek techniczny, a następnie prezentował uzasadnienie ze wskazaniem podstawy, na jakiej opiera wniosek o braku spełnienia danego wymagania. Tylko te kwestie, które zostały w uzasadnieniu poruszone, wyznaczały zakres rozpoznania. Należy odnotować, iż złożenie odpowiedzi na odwołanie nie otwierało drogi do formułowania zarzutów szerzej, niż miało to miejsce w odwołaniu. Odpowiedź Zamawiającego, jak i stanowisko Przystępującego były reakcją na argumenty i kwestie techniczne wskazane w odwołaniu, które w ocenie Odwołującego miały uzasadniać

twierdzenie o braku zgodności z wymaganiami zamówienia. Jeżeli odpowiedzi te prowokowały dalszą dyskusję wykraczającą poza podstawę faktyczną zarzutu, nowe okoliczności nie były brane pod uwagę przy rozpoznaniu

odwołania, nawet jeżeli miały odniesienie do konkretnego, wskazanego w odwołaniu warunku (co zostanie odpowiednio odnotowane w dalszej części uzasadnienia). Należy również zauważyć, iż przedmiot zamówienia i wymagania opisane przez Zamawiającego uwzględniały oczekiwania wobec działania i funkcjonalności systemu. Zatem dla ustalenia na jakiej podstawie Odwołujący wnioskuje o braku spełnienia wymagań decydowało uzasadnienie i wskazanie na te elementy oferowanego rozwiązania, które miały prowadzić do stwierdzenia, w jakim zakresie funkcjonalność nie może być osiągnięta. Nie wystarczyło zatem samo zacytowanie opisu przedmiotu zamówienia, bez odniesienia do konkretnej okoliczności pozwalającej ocenić, czy produkt spełnia wymagania Zamawiającego.

Przechodząc zatem do kwestii szczegółowych objętych zarzutami, stanowisko Izby podzielone zostanie na dwie części, odnosząc się do dwóch ofert.

I . Zarzuty dotyczące oferty wybranej – IT Solution Factor Sp. z o.o. (dalej jako IT Solution) Izba w całości oddaliła.

W pierwszej kolejności Izba uznała, iż ocena produktu zaoferowanego w ofercie IT Solution, tj. Trend Vision One – Endpoint Security (Essentials) producenta Trend Micro, w części w jakiej Odwołujący opierał na twierdzeniu, iż zawiera ono dwa produkty do ochrony Endpoint, tj. „Standard Endpoint Protection – ochrona desktopów: Windows, macOS" oraz „Serwer and Workload Protection – ochrona serwerów: Windows, Linux", posiadające osobne agenty, konsole zarządzające, polityki i funkcjonalności, oparta była na błędnym przekonaniu własnym Odwołującego o produkcie. Odwołujący w żaden sposób nie skomentował oficjalnych informacji o produkcie, który objęty jest jedną licencją oprogramowania Trend Vision One. Jako rozwiązanie chmurowe obejmuje dwie funkcjonalności (wskazane przez Odwołującego w sposób nieuprawniony jako „dwa produkty"), tworzące jedno rozwiązanie licencyjne i umożliwiające uruchomienie ochrony w ramach jednej centralnej konsoli Trend Vision One. Zamawiający powołał się na oficjalne informacje producenta, których Odwołujący nie podważył, a tym samym odwołanie w zakresie argumentów opartych na wykazaniu rozdzielnych funkcjonalności „Standard Endpoint Protection" oraz „Serwer and Workload Protection", które miały być dostępne z poziomu oddzielnych konsol, nie miały oparcia w rzeczywistości. Tym samym wnioski o niezgodności produktu z wymaganiami oparte na tej okoliczności Izba uznała za bezzasadne (zarzut nr 1 i kolejne odpowiednio wskazane poniżej).

Przechodząc do poszczególnych parametrów Izba odniesie się oddzielnie do każdego z zarzutów w kolejności odpowiadającej treści odwołania.

- rozdział II OPZ, pkt 4.3 – wymóg: „Automatyczna Reakcja i Izolacja Zagrożeń musi posiadać: „zestaw silników które można włączać lub wyłączać;"

W rozwiązaniu, zdaniem Odwołującego, nie można wyłączyć silników jako automatyczna reakcja ani podczas izolacji zagrożeń. Wszystkie możliwe czynności dla automatycznej reakcji i izolacji zagrożeń Odwołujący przedstawił na zrzucie ekranu z oferowanych rozwiązań Tren Micro. Nie ma tu możliwości wyłączania lub włączania zestawu silników czego wymaga Zamawiający.

Zamawiający Przystępujący wskazali na możliwość użycia funkcjonalności programu tzw. playbook, pozwalającej na wykorzystanie skryptu do wyłączenia/włączenia dowolnego zestawu silników.

Izba oddaliła zarzut uznając, iż zrzut z ekranu przedstawiony w odwołaniu nie prezentuje innych dostępnych funkcjonalności systemu, pozwalających na włączanie/wyłączanie silników (playbook, skrypty). Jednocześnie słusznym jest argument Przystępującego, iż w OPZ nie zostały wskazane zestawy silników, dla których konkretnie wymóg ten się odnosi, jak również z jakiego poziomu funkcjonalność ta ma być zagwarantowana.

- rozdział II OPZ, pkt 4.5 – wymóg: „możliwość przeniesienia do kwarantanny złośliwych plików należących do tego samego incydentu. Funkcja kwarantanny musi zatrzymać procesy, szyfrować plik wykonywalny i przenieść go na ograniczoną ścieżkę;"

Zdaniem Odwołującego, oferowane rozwiązania Trend Micro nie zawierają opcji przeniesienia wszystkich plików z incydentu do kwarantanny. Pliki w incydencie można dodać do listy blokowania (zrzut z ekranu), co nie jest jednoznaczne z kwarantanną, dodawać pliki można tylko pojedynczo. W dostępnych opcjach oferowane rozwiązanie nie posiada możliwości przeniesienia do kwarantanny złośliwych plików należących do tego samego incydentu czego wymaga Zamawiający.

Izba oddaliła zarzut, jako niezasadny. Nie budziło sporu, iż funkcja dodawania do listy blokowania nie oznacza jeszcze przeniesienia do kwarantanny złośliwych plików. Jednocześnie odwołujący sam przyznał na rozprawie, iż system ma funkcję kwarantanny, kwestionując przy tym prezentowane przez przeciwników sporu zrzuty z ekranu prezentujące tą funkcjonalność, którą poprzedza akcja dodawania do listy blokowanych. Należy wskazać, iż Zamawiający nie narzucił konkretnego schematu w jakim dany system ma dodawać pliki z incydentu do kwarantanny, a tym samym rozwiązanie zaoferowane nie jest niezgodne z wymaganiem, gdyż posiada możliwość przeniesienia do kwarantanny złośliwych plików należących do tego samego incydentu. Z wyjaśnień Przystępującego i Zamawiającego

wynika, że prezentowane przez nich zrzuty obrazują sposób przeniesienia do kwarantanny plików w sposób automatyczny lub pojedynczo przez dodanie do listy blokowania. Odpowiedź Odwołującego udzielona na pytanie o przedstawione mechanizmy nie przekonała, gdyż w ogóle nie kwestionuje możliwości przeniesienia do kwarantanny. Na rozprawie Odwołujący próbował rozszerzyć zarzut na ocenę samego incydentu, a nie funkcjonalności dodawania do kwarantanny, co Izba pominęła.

- rozdział II OPZ, pkt 5.1 – wymóg: „Jedno plikowy agent AV, który musi być w pełni autonomiczny, co oznacza,

że jego działanie i funkcjonalność nie może być zależna od serwera zarządzania, chmury ani ŻADNYCH zasobów zewnętrznych od agenta;”

W ocenie Odwołującego, brak Internetu uniemożliwia działanie funkcjonalności: behavior monitoring (tłumaczenie z ang.: monitorowanie/analiza behawioralna), predictive machine learning (tłumaczenie z ang.: predyktywne uczenie maszynowe), i process memory scanning (tłumaczenie z ang.: skanowanie procesów w pamięci).

Izba na podstawie wskazanych w pismach mechanizmów działania uznała, iż stanowisko Odwołującego wynika z wybiórczej oceny działania automatycznego agenta AV, które nie uwzględnia mechanizmów pozwalających na niezależne od serwera jego działanie. Zamawiający wskazał na możliwości jakie stwarza wykorzystanie paczki „web instaler” lub skryptu. Ponadto, Odwołujący wybiórczo zacytował treść dokumentacji, tj. z pominięciem tej części, w której podane są dostępne rozwiązania w sytuacji gdyż agent nie działa (str. 7 pisma Przystępującego). Tym samym twierdzenia o braku możliwości działania niezależnie od zasobów zewnętrznych, nie zostało przez Odwołującego wykazane. Wybiórcza analiza rozwiązania nie może stanowić uzasadnienia dla uznania, iż rozwiązanie nie spełnia warunku. Ponadto, same funkcje systemu wybiórczo wskazane w tym miejscu odwołania są dostępne, co potwierdzają zrzuty z ekranu w odpowiedzi na odwołanie, a Zamawiający opisując warunek nie odnosił się do konkretnych funkcjonalności, ale działania samego agenta AV, w pełni autonomicznego.

- rozdział II OPZ, pkt 5.9.2, wymóg: „funkcjonalność automatycznej aktualizacji, która musi pozwalać na wybór stacji końcowych które powinny zostać zaktualizowane posiadając możliwość wyboru co najmniej: jedynie stacji końcowych z wybranym tag-iem;”

Odwołujący wskazał, iż Standard Endpoint Protection Manager posiada tagowanie endpointów, ale nie ma możliwości definiowania aktualizacji na podstawie tagów. Server and Workload Protection Manager ma tagi tylko dla zdarzeń/logów, nie ma dla endpointów.

Zarzut podlegał oddaleniu, gdyż wynikał z błędnego przedstawienia produktu, jako składającego się z dwóch oddzielnych, wymagających dwóch konsoli obsługujących ich funkcjonalności. Aktualne w tym zakresie pozostaje stanowisko wyrażone na wstępie

uzasadnienia o braku podstaw dla uznania zarzutów wywodzonych z takiej analizy zaoferowanego rozwiązania. Przedstawione w kontrze zrzuty z ekranu prezentują funkcje tagowania dla stacji końcowej. Przystępujący wyjaśniał działanie mechanizmu wykorzystującego etykiety przypisane stacji końcowej, które pozwalają na aktualizację tylko dla określonych etykietami stacji (otagowane). Obrazują to również przedstawione w piśmie procesowym Przystępującego kroki (str. od 8 do 11). Argumenty Odwołującego dotyczące tagowania, jako obrazującego „wpisanie z palca”, a nie efekt nadania etykiety, były w ocenie składu orzekającego oderwane od rzeczywistości i stanowiły autorską ocenę prezentowanych działań zakończonych nadaniem etykiety.

- rozdział II, pkt 5.12, wymóg: „możliwość zdefiniowania maksymalnej liczby stacji końcowych pobierających jednocześnie paczkę aktualizacyjną;”

W ocenie Odwołującego, oferowane rozwiązanie nie ma takiej opcji.

Izba oddaliła zarzut jako gołosłowny, oderwany od faktycznych mechanizmów działania systemu, w którym administrator może określić zarówno wszystkie stacje końcowe jak i stacje końcowe należące do konkretnej grupy, co jest powiązane z funkcją tagowania stacji końcowych, dla których nastąpi pobranie aktualizacji. Ograniczenie liczby stacji nie musi odbywać się wyłącznie przez wskazanie ich liczby, ale zapewnione jest również przez wskazanie grupy zawierającej wszystkie stacje o ustalonej etykiecie (tagu). Nie jest to jedyny sposób zdefiniowania maksymalnej liczby stacji końcowych, do czego odnosi się Przystępujący w piśmie procesowym (str. 11-17). Należy również podkreślić, iż zarzut w zasadzie sprowadzał się do zaprzeczenia działania tej możliwości i wskazania wybranego przez Odwołującego screenu. Argumentacja nie została w żaden sposób rozwinięta i nie odnosi się do innych możliwych działań administratora, pozwalających na zdefiniowanie maksymalnej liczby stacji, co zostało przedstawione merytorycznie dopiero przez Przystępującego i Zamawiającego. Odwołujący dopiero w piśmie procesowym rozszerzał argumentację o znaczenie pojęcia „zdefiniowanie maksymalnej liczby” nadając mu znaczenie jako możliwość podania/ustawienia maksymalnej liczby, dla której aktualizacja będzie miała zastosowanie. Skład orzekający taki sposób rozumienia traktuje jako możliwy ale nie jedyny, w świetle specyfiki przedmiotu zamówienia i różnych metod pozwalających ograniczyć liczbę stacji końcowych bez narzucania na sztywno ich liczby. Ograniczenie zbioru stacji końcowych np. wskazaną etykietą (tagiem) będzie formą zdefiniowania maksymalnej liczby stacji mieszczących się w zbiorze, co spełnia warunek swz. Za takim rozumieniem przemawia fakt, iż Zamawiający nie narzucił z góry na sztywno konkretnej maksymalnej liczby stacji końcowych, dla których jednocześnie pobrana miałaby być aktualizacja. Taki opis wymagania nie ingeruje w różne rozwiązania stosowane przez producentów, co mogłoby istotnie ograniczać konkurencję. Możliwość zdefiniowania

maksymalnej liczby stacji nie może być ograniczana w taki sposób jak rozumie to Odwołujący, gdyż prowadzi do zawężenia znaczenia funkcjonalności, która kładzie nacisk na samo zdefiniowanie, a więc sposób określenia maksymalnej liczby, co nie może być zrównywane wyłącznie z wprowadzeniem liczby maksymalnej.

- rozdział II OPZ, pkt 5.18, wymóg: „informacje dla każdego pakietu instalacyjnego, które muszą zawierać co najmniej następujące dane:

5.18.1 wersja główna,

5.18.2 numer buildu,

5.18.3 rozszerzenie pliku,

5.18.4 nazwa pliku,

5.18.5 data opublikowania,

5.18.6 platforma”

W ocenie Odwołującego powyższe informacje nie są wyświetlane w Standard Endpoint Protection Manager, a w Server and Workload Protection Manager nie ma „daty opublikowania”. W kolumnach tabeli zawierającej pakiety instalacyjne są kolumny „Nazwa”, „Platforma”, „Wersja”, „Typ publikacji” i „Data importu”. Nie istnieje kolumna „Data opublikowania” czego wymaga Zamawiający. Data importu jest myląca dla administratorów, ponieważ może być różna dla tego samego pakietu (np. przy ponownym pobraniu) i niezgodna chronologicznie w porównaniu z datą opublikowania, np. starszy pakiet instalacyjny może być zaimportowany później niż nowszy. Data opublikowania jest niezmienna i niezależna od momentu pobrania pakietu instalacyjnego.

Izba oddaliła zarzut, gdyż wynikał z błędnego przedstawienia produktu, jako składającego się z dwóch oddzielnych, wymagających dwóch konsoli obsługujących ich funkcjonalności. Aktualne w tym zakresie pozostaje stanowisko wyrażone na wstępie uzasadnienia o braku podstaw dla uznania zarzutów wywodzonych z takiej analizy zaoferowanego rozwiązania. Ponadto, Zamawiający i Przystępujący wykazali, iż wskazane informacje zawierają wymagane dane. Szczególną uwagę Odwołujący skupiał na „dacie publikacji” przedstawiając jako dowód informacje o produkcie Deep Security.

Izba oddaliła zarzut uznając wyjaśnienia Zamawiającego i Przystępującego za spójne i przekonujące. Odwołujący faktycznie odwołał się do daty publikacji agenta dla produktu, który nie jest oferowany i wymaga pobrania ze strony, co wiąże się z tym, że data importu nie jest datą publikacji. W przypadku zaoferowanego produktu, który jest chmurą jednocześnie z publikacją przez producenta agent jest dostępny (importowany), gdyż jest to jedno zdarzenie. Nie ma zatem podstaw do podważania informacji przedstawionych na screenach dotyczących zaoferowanego produktu.

- rozdział II OPZ, pkt 6.10, wymóg: „możliwość stopniowania poziomu wyjątków dla wyjątków typu "Ścieżka" w systemie Windows , co najmniej w następującym zakresie:

6.10.1 wygaszenie alarmów,

6.10.2 zredukowanie monitorowania konkretnego procesu,

6.10.3 zredukowanie monitorowania konkretnego procesu i jego procesów potomnych,

6.10.4 wyłączenie monitorowania konkretnego procesu,

6.10.5 wyłączenie monitorowania konkretnego procesu i jego procesów potomnych;”

W ocenie Odwołującego, oferowane rozwiązania Trend Micro nie spełniają tego zapisu opcji 6.10.1 do 6.10.5 dla ścieżki/path systemu Windows, co przedstawiono na zrzutach ekranu. Na zrzutach ekranu widoczne są opcje konfiguracji wyjątków typu „ścieżka” w systemie, nie ma jednak opcji przedstawionych w podpunktach 6.10.1 do 6.10.5 czyli możliwości określenia stopnia poziomu wyjątku tego typu. Zrzuty ekranów pochodzą z konfiguracji polityki w produktach ochrony antymalware. Funkcjonalność XDR jest osobna i niezależna od produktów Standard Endpoint Protection Manager i Server and Workload Protection Manager. W konsoli oferowanych rozwiązań Trend Micro, w opcjach wykrywania zagrożeń za pomocą XDR są opcje 6.10.1, 6.10.4, 6.10.5. Podpunkt 6.10 należy do punktu „6. Zarządzanie Politykami Bezpieczeństwa musi uwzględnić:” czyli do ustawień polityk. Jeżeli w wykrywaniu zagrożeń za pomocą telemetrii XDR zostaną wprowadzone wyjątki, to nie będą one działać podczas wykrywania zagrożeń bezpośrednio w produktach Standard Endpoint Protection Manager i Server and Workload Protection Manager czyli w rzeczywistym oprogramowaniu antywirusowym. Dlatego wyjątki możliwe do wprowadzenia w produkcie XDR nie powinny być brane pod uwagę. Jednak nawet, uwzględniając opcje wyjątków w produkcie XDR, nie są spełnione punkty 6.10.2, 6.10.3.

Zamawiający w odpowiedzi na zarzut wskazał trzy poziomy, na jakich stopniowanie wyjątków i ich tworzenie może odbywać się w oprogramowaniu Trend Vision One. Również Przystępujący w piśmie procesowym przedstawił przykład ścieżki prezentujący konfigurację zredukowania monitorowania konkretnego procesu i jego procesów potomnych (notepad.exe), polegający na dodaniu dodatkowego warunku (st. 21-25).

Izba oddaliła zarzut, jako bezpodstawny. Twierdzenia Odwołującego nie mają odniesienia do funkcjonalności oprogramowania Trend Vision One, wskazanych w pismach Zamawiającego i Przystępującego. Pomimo wykazania możliwości wprowadzenia dodatkowych warunków pozwalających na zidentyfikowanie konkretnego procesu, Odwołujący stał na stanowisku, iż takiej możliwości nie ma. Nie zostało ono w żaden sposób wykazane, co prowadziło do oddalenia zarzutu. Ocena funkcjonalności opisanej w pkt 6.10 nie może być sprowadzona do wybiórczego przedstawiania elementów procesów, które nie dają całościowego obrazu działania zaoferowanego systemu. Stanowisko Odwołującego ponownie sprowadzone

zostało do wydzielenia, jako elementów systemu produktów Standard Endpoint Protection Manager i Server and Workload Protection Manager i nie uwzględnia funkcjonalności całego produktu i jego działania.

- rozdział II OPZ, pkt 6.11, wymóg: „rozwiązanie, dla wyjątków typu "Ścieżka" w systemie Linux musi mieć możliwość stopniowania poziomu wyjątków, co najmniej w następującym zakresie:

6.11.1 wygaszenie alarmów,

6.11.2 wyłączenie monitorowania konkretnego procesu”

W ocenie Odwołującego oferowane rozwiązania Trend Micro nie spełniają tego zapisu. Nie ma opcji 6.11.1 i 6.11.2 dla ścieżki/path systemu Linux co przedstawiono na zrzutach ekranu Zrzuty ekranów pochodzą z konfiguracji polityki w produktach ochrony antymalware. Funkcjonalność XDR jest osobna i niezależna od produktów Standard Endpoint Protection Manager i Server and Workload Protection Manager. Opcje opisane w punktach 6.11.1 i 6.11.2 są tylko dostępne w wyjątkach wykrywania zagrożeń za pomocą XDR, nie dla antywirusa/polityki agenta. Podpunkt 6.10 należy do punktu „6. Zarządzanie Politykami Bezpieczeństwa musi uwzględnić:” czyli do ustawień polityk a w ustawieniach polityki nie ma opisanych opcji. Jeżeli w wykrywaniu zagrożeń za pomocą telemetrii XDR zostaną wprowadzone wyjątki, to nie będą one działać podczas wykrywania zagrożeń bezpośrednio w produktach Standard Endpoint Protection Manager i Server and Workload Protection Manager czyli w rzeczywistym oprogramowaniu antywirusowym. Dlatego wyjątki możliwe do wprowadzenia w produkcie XDR nie powinny być brane pod uwagę.

Z uwagi na tożsamość z zarzutem dotyczącym spełnienia wymagań z pkt 6.10, rozdział II OPZ, Izba podtrzymuje stanowisko przedstawione powyżej i oddala w tym zakresie odwołanie.

- rozdział II OPZ, pkt 6.18, wymóg: „moduł kontroli sieci, który musi być zintegrowany z funkcjonalnością tagowania hostów w oferowanym rozwiązaniu”

Oferowane rozwiązania Trend Micro nie spełniają tego wymagania. Standard Endpoint Protection Manager posiada tagowanie endpointów ale nie można ich wykorzystać w module kontroli sieci. Server and Workload Protection Manager posiada tagi tylko dla zdarzeń/logów, nie ma tagowania dla endpointów. Nie ma integracji modułu kontroli sieci z tagowaniem hostów. Możliwość tagowania ograniczająca się tylko do zdarzeń/logów w produkcie Server and Workload Protection Manager przedstawiono na zrzutach ekranu.

Tylko dla zdarzeń, które na zrzucie są widoczne jako kolejne rzędy, można dodać tag („Add Tag(s)”).

Odwołujący formułując tezę o braku spełnienia parametru ponownie odrębnie traktuje produkty Standard Endpoint Protection Manager i Server and Workload Protection Manager, co nie przedstawia pełnej funkcjonalności zintegrowanego rozwiązania zaoferowanego i nie mogło przesądzać o niezgodności oferty z swz. Ponownie Odwołujący w sposób dowolny przedstawia tagowanie, jako, co w ocenie składu orzekającego nie może być wykazane przez wybiórczą analizę elementów systemu.

- rozdział II OPZ, pkt 6.20, wymóg: „interfejs graficzny modułu kontroli sieci, który musi oferować możliwość importowania wybranych wyjątków dla kwarantanny sieciowej rozwiązania z pliku .json.”

W ocenie Odwołującego rozwiązania Trend Micro potrafią jedynie zaimportować plik z formatu XML co przedstawiają zrzuty ekranu z konsoli Trend Micro. Pokazują one możliwość eksportu reguł, w tym wyjątków czyli reguł dopuszczających ruch, do formatu możliwego do zaimportowania w postaci XML, tj. „Export to XML (For Import)” czyli „Eksport do formatu XML (na potrzeby importu)” oraz „Export Selected to XML (For Import)” czyli „Eksport wybranych reguł do formatu XML (na potrzeby importu)”. XML to odmienny format pliku niż JSON. Posiada inną strukturę wewnętrzną. JSON (JavaScript Object Notation) to otwarty standardowy format tekstowy do wymiany danych. Podczas przetwarzania informacji JSON wykorzystuje mniej pamięci niż XML co powoduje, że JSON jest lepszym formatem do szybkiego przetwarzania dużych ilości danych. Nie jest możliwe zastosowanie tego samego analizatora składniowego (parsera) do obu formatów jednocześnie co sprawia, że formaty JSON i XML nie są zamienne.

Zamawiający w odpowiedzi wskazał na możliwość wykorzystania playbooka korzystającego z dostępnych funkcji API, który pozwala przekonwertować każdy format, w tym format XML do pliku .json. Sposób konfiguracji playbooka z interfejsu graficznego przedstawił Przystępujący w piśmie procesowym na str. od 29 do 31.

Izba oddaliła zarzut przyjmując, że opisany wymóg nie dyskwalifikuje rozwiązania wykorzystującego skrypt, jako elementu funkcjonalności całego rozwiązania. Nie można w ocenie Izby w sposób wybiórczy badać funkcjonalności. Zamawiający nie wyłączył możliwości wykorzystania skryptów (PowerShell, Bash), w celu importowania wyjątków dla kwarantanny sieciowej z pliku .json.

- rozdział II OPZ, pkt 7.12, wymóg: rozwiązanie musi mieć możliwość filtrowania stacji końcowych na których został zainstalowanych agent, co najmniej z wykorzystaniem następujących parametrów: (...) – wskazane w pkt 7.12.1-7.12.17.

W ocenie Odwołującego rozwiązania Trend Micro nie spełniają punktów 7.12.2 (tag przypisany do stacji końcowej), 7.12.6 (domena MS Windows), 7.12.9 (stan sieci stacji

końcowej), 7.12.15 (jakikolwiek ciąg znaków z domeny Microsoft Windows). Zrzuty ekranu pochodzą z różnych konsol zarządzania, punkty, które nie są spełnione dotyczą wszystkich konsol. W każdej z konsol jest tylko część wymienionych parametrów.

Izba oddaliła zarzut, który opierał się na błędnym wydzieleniu jako odrębnych produktów elementów systemu

oferowanego. Odwołujący ponownie w tym miejscu traktuje oddzielnie konsole wyróżniając ich parametry, co nie uwzględnia faktu, iż zaoferowanym system stanowi zintegrowane rozwiązanie zarządzane z poziomu jednej wspólnej konsoli zarządzania.

- rozdział II OPZ, pkt 7.15, 7.16, 7.19 – wymagania: „7.15 rozwiązanie musi umożliwiać oznaczanie hostów poprzez etykiety (tagi); 7.16 każda etykieta (tag) musi być określana poprzez parametr - nazwa etykiety (tagu); 7.19 rozwiązanie musi umożliwiać dopisanie wielu etykiet (tagów) do jednej stacji końcowej;“

Odwołujący wskazał, iż Standard Endpoint Protection Manager posiada tagowanie endpointów ale nie obsługuje serwerów Linux, które są wymagane do obsługi zgodnie z wymaganiami OPZ, np. Rozdział II, punkt 5.6. „możliwość automatycznej aktualizacji agentów zainstalowanych na stacjach końcowych z systemem operacyjnym: Microsoft Windows oraz Linux;”. Server and Workload Protection Manager posiada tagi tylko dla zdarzeń/logów, nie posiada tagów dla hostów/stacji końcowych. Możliwość tagowania ograniczająca się tylko do zdarzeń/logów w produkcie Server and Workload Protection Manager przedstawiona została na zrzutach ekranu z konsoli rozwiązań Trend Micro.

Izba oddaliła zarzut, który opierał się na błędnym wydzieleniu jako odrębnych produktów elementów systemu oferowanego. Odwołujący ponownie w tym miejscu traktuje oddzielnie konsole wyróżniając ich parametry, co nie uwzględnia faktu, iż zaoferowanym system stanowi zintegrowane rozwiązanie zarządzane z poziomu jednej wspólnej konsoli zarządzania. Ponadto, Odwołujący w sposób dowolny nadaje znaczenia pojęciu „tagowanie”, jako opisywanie, wskazując również na brak precyzyjnego określenia w dokumentacji Trend Vision One czym są tagi i w jaki sposób można je dodać do hostów. W ocenie składu pojęcie to jako przypisane i zrozumiane w branży nie wymaga szczegółowego omawiania i samo wskazanie na TGA na zrzutach ekranów pozwala uznać, iż system oznacza hosty poprzez etykiety (tagi).

- rozdział II OPZ, pkt 8.9, wymóg: „interfejs graficzny modułu kontroli sieci, który musi prezentować reguły w formie tabularycznej, z możliwością definiowania następujących kolumn:

8.9.1 nazwa,

8.9.2 opis,

8.9.3 aplikacja,

8.9.4 poziomami struktury rozwiązania, dla których reguły są aplikowane,

8.9.5 system operacyjny,

8.9.6 status (włączona / wyłączona),”

Oferowane rozwiązania Trend Micro, w ocenie Odwołującego nie spełniają punktów 8.9.3 do 8.9.6, co zostało zaprezentowane na zrzutach ekranu z konsoli. Zrzuty ekranu przedstawiają wszystkie możliwe do zdefiniowania kolumny prezentowanych reguł w formie tabelarycznej interfejsu graficznego modułu kontroli sieci. Oferowany produkt nie posiada możliwości definiowania kolumn wyszczególnionych w punktach 8.9.3 do 8.9.6.

Zamawiający i Przystępujący w odpowiedzi na ten zarzut przedstawili zrzut z systemu Trend Micro One moduł kontroli sieci, prezentujący w formie tabelarycznej kolumny z danymi. Odwołujący podważając informacje prezentowane przez oponentów sugerował, iż określenia FTP nie musi identyfikować aplikacji, ale porty na jakich działa i w zależności od ustawień serwera świadczącego usługę FTP będzie odzwierciedlać ustawienia domyślne.

Tłumaczenie Odwołującego nie przekonało do uznania, iż rozwiązanie nie spełnia wymagań dotyczących możliwości definiowania kolumn. Przedstawione w piśmie procesowym Przystępującego zrzuty z systemu Trend Micro Vision One przekonały skład, iż są to dane przedstawiane przez producenta, odpowiadające wymaganiom. Odwołujący podjął w piśmie procesowym polemikę, która istotnie wykraczała poza zarzut, w którym kwestionował sam brak możliwości definiowania kolumn w zakresie wyszczególnionym w pkt 8.9.3 do 8.9.6. Odwołujący odnosił się do wybranej reguły DNS Server, w której poziomy struktury nie jest prezentowane w formie tabularycznej. W ocenie Izby nie podważało to informacji prezentowanych w pismach Zamawiającego i Przystępującego określających poziom struktury rozwiązania, jak i system operacyjny (Windows, Linux).

- rozdział II OPZ, pkt 9.4, wymóg: „zakres czasu raportów, który musi być możliwy do zdefiniowania przez użytkownika konsoli zarządzającej;”

W opinii Odwołującego, w oferowanych rozwiązaniach Trend Micro użytkownik nie może zdefiniować zakresu, może tylko wybrać zakres z listy zdefiniowanej przez producenta, w przypadku raportów z harmonogramu (Scheduled report), jest to lista zdefiniowanej przez producenta z opcjami dzień, tydzień, miesiąc, w przypadku jednorazowych raportów (One time report), jest to lista z opcjami 7 dni, 30 dni. Przedstawiono zrzuty, które opisują konfiguracje, w których brakuje możliwości zdefiniowania zakresu. Podczas prazy z innymi funkcjonalnościami istnieje możliwość definiowania zakresu czasu, np. dla wyszukiwania zdarzeń w funkcjonalności XDR. Przedstawiono na zrzucie ekranu możliwość wyboru definiowanego zakresu (Custom period) w wyszukiwaniu zdarzeń XDR. Można wybrać dzień

i godzinę, od której („From:”) oraz do której („To:”) wyszukiwanie będzie obowiązywać. Podczas tworzenia raportów rozwiązanie nie daje takiej możliwości więc nie spełnia cytowanego wymagania, którego spełnienia wymaga Zamawiający.

Przystępujący w piśmie procesowym wskazał na funkcję Custom Range, w której istnieje możliwość wybrania dowolnego okresu za jaki ma być wygenerowany raport (w przykładzie – ostatnie 7 dni, jak również możliwość wskazania przedziałem czasowym).

Powyższe zdaniem składu orzekającego wskazuje na bezzasadność zarzutu. Dalsza argumentacja Odwołującego, w tym dotycząca miejsca w którym wygenerowane raporty muszą być dostępne, wykraczała poza podstawę zarzutu. Ponadto, sam Zamawiający nie określał miejsca, w jakim raport ma być generowany.

- rozdział II OPZ, pkt 10.14, wymóg: „moduł zarządzania aktywnościami, który musi oferować możliwość filtrowania logów w następujących kategoriach:

10.14.1 odpowiedź na zagrożenia;

10.14.2 zarządzanie incydentami;

10.14.3 wykluczenia;

10.14.4 operacje administratorskie;

10.14.5 email użytkownika konsoli;

10.14.6 nazwa hosta."

W ocenie Odwołującego rozwiązanie nie posiada filtrowania logów w kategoriach 10.14.1, 10.14.2, 10.14.3, 10.14.5, co przedstawiono na zrzutach ekranu z konsoli oferowanych

rozwiązań Trend Micro.

Odwołujący kwestionował argumenty Zamawiającego podnosząc, iż prezentowane w odpowiedzi na odwołanie powiadomienia generowane w systemie nie pochodziły z modułu zarządzania aktywnościami. Jednocześnie Odwołujący w żaden sposób nie skomentował twierdzenia i przykładu przedstawionego w piśmie Przystępującego (str. 44 do 48), który wprost odnosi się do akcji będących odpowiedzią na zagrożenia, pochodzących wprost modułu zarządzania, na co wskazuje dziennik logowania administratora z poziomu konsoli.

W ocenie składu orzekającego zarzut nie miał podstaw i wynikał z autorskiego przedstawienia działania systemu wybiórczo prezentowanego w odwołaniu. Należy również odnotować, iż w uzasadnieniu tego i wielu innych punktów w odwołaniu stanowisko Odwołującego sprowadzało się wyłącznie do zakwestionowania danej funkcjonalności i przedstawienia wybranego na potrzeby konkretnego parametru obrazu. Dopiero w replice na stanowiska procesowe Odwołujący szeroko komentował inne wskazane drogi i narzędzia pozwalające ocenić pozytywnie rozwiązania przyjęte w systemie Trend Micro Vision. W ocenie składu orzekającego taka taktyka prowadzenia sporu prowadzi często do

wykroczenia poza zakres okoliczności wskazanych w odwołaniu i nie może być skutecznie prowadzić do rozszerzenia podstawy faktycznej. Jak Izba wskazywała na wstępie, w przypadku kwestionowania danej funkcjonalności i odniesienia się do wybranego jej elementu, nie można na etapie rozprawy skutecznie twierdzić, iż zarzut obejmuje pełen zakres funkcjonalności wynikający z cytowanych zapisów OPZ. Tylko w takim zakresie w jakim Odwołujący odniesie się w odwołaniu do konkretnego rozwiązania, jest możliwość prowadzenia sporu i prezentowania stanowisk. Słusznie zatem Zamawiający wskazał, iż przygotowując odpowiedź na odwołanie kierował się kwestiami podniesionymi w podstawie faktycznej, wskazując na takie elementy systemu, które odpierały zarzut. Dalsza polemika o tych elementach nie mogła zatem prowadzić do podnoszenia nowych kwestii, nie poruszonych w samym zarzucie i jego uzasadnieniu faktycznym.

- rozdział II OPZ, pkt 10.15, wymóg: „moduł zarządzania aktywnościami, który musi oferować możliwość eksportowania wpisów 100, 1000, 5000 lub 10000 ostatnich aktywności do pliku .csv."

Odwołujący wskazał, iż dla modułu zarządzania aktywnościami nie ma możliwości eksportu określonej liczby wpisów, czego wymaga Zamawiający i co jest przedstawione na zrzutach ekranu z konsoli oferowanych rozwiązań Trend Micro. Po wybraniu opcji „Export as .csv file." czyli „Eksportuj jako plik .csv" eksportowane są wszystkie wyświetlone wpisy.

W odpowiedzi na tak postawiony zarzut Zamawiający i Przystępujący przedstawili zrzuty prezentujące możliwości pobierania logów przez agenta końcowego dla przykładowych ilości wpisów 50, 100 lub 200.

W ocenie Izby wykazana ilość wpisów 100 potwierdza wymóg Zamawiającego. Ilość ta wprost referuje do wymagania z pkt 10.15.

- rozdział II OPZ, pkt 10.16, wymóg: „moduł zarządzania aktywnościami, który musi oferować możliwość pobierania logów zebranych przez agenta końcowego po wydaniu komendy z poziomu modułu zarządzania;"

W ocenie Odwołującego moduł zarządzania aktywnościami (Audit Log) nie ma takiej opcji, co potwierdzać ma zrzut ekranu z konsoli oferowanych rozwiązań Trend Micro. Na zrzucie ekranu z modułu zarządzania aktywnościami (Audit Log) jedynymi dostępnymi opcjami jest filtrowanie wpisów i eksportowania ich jako pliku CSV.

Przystępujący i Zamawiający przedstawili możliwości modułu zarządzania z wykorzystaniem funkcji get events, służącej zbieraniu logów przez agenta końcowego (oprogramowanie zainstalowane na stacji administratora).

Samo zaprzeczenie przez Odwołującego możliwości systemu nie jest wystarczające dla podważenia funkcjonalności oprogramowania. Izba oddaliła na tej podstawie zarzut jako bezpodstawny.

- rozdział II OPZ, pkt 10.23, wymóg: „zarządzanie notyfikacjami, które musi umożliwiać wyszukiwanie pojedynczego rodzaju zdarzenia poprzez wyszukiwarkę tekstową;" Odwołujący przedstawił zrzut z ekranu, na którym nie ma okna lub sekcji, w której można przeprowadzić wyszukiwanie powiadomień. Jest dostępna lista powiadomień ale nie można ich wyszukać poprzez wyszukiwarkę tekstową.

Zamawiający i Przystępujący przedstawili możliwości, jakie daje wyszukiwarka tekstowa dla wyszukiwania pojedynczego zdarzenia.

Izba oddaliła odwołanie, jako mające uzasadnienie wyłącznie w wybiórczej analizie rozwiązania, posiadającego możliwość wyszukiwania pojedynczego zdarzenia poprzez wyszukiwarkę tekstową. Argumenty Odwołującego nie podważają przykładów działania systemu wykazane w pismach procesowych Zamawiającego i Przystępującego.

- rozdział II OPZ, pkt 10.24, wymóg: „10.24 zarządzanie notyfikacjami, które musi wyróżniać następujące typy powiadomień:

10.24.1 administracyjne;

10.24.2 kontrola urządzeń;

10.24.3 tagi urządzeń;

10.24.4 kontrola firewall;

10.24.5 malware;

10.24.6 łagodzenie incydentów;

10.24.7 operacje;

10.24.8 Remote Shell;"

Odwołujący kwestionuje spełnienie wymagań w zakresie podpunktów 10.24.3, 10.24.6 oraz 10.24.8, co przedstawiono na zrzucie ekranów z konsoli oferowanych rozwiązań Trend Micro. Zrzuty ekranów przedstawiają miejsca, w których można konfigurować notyfikacje. Ponieważ oferta składa się z wielu produktów, konfiguracja notyfikacji nie jest możliwa w pojedynczym panelu. Na zrzutach ekranów przedstawiono wszystkie możliwe do skonfigurowania notyfikacje.

Izba oddaliła zarzut oparty na rozróżnieniu, jako dwóch niezależnych produktów, jak również odmiennego rozumienia tagowania, które Odwołujący nadaje w odwołaniu. Argumenty Odwołującego nie były wystarczające dla podważenia możliwości, jakie zostały wykazane w pismach procesowych Zamawiającego (str. 39, 40) i Przystępującego (str. 53-55).

II. Zarzuty dotyczące oferty złożonej przez Trafford IT

Zgodnie ze złożoną ofertą, Trafford IT, zaoferowało oprogramowanie Cortex XDR producent Palo Alto Networks.

W ocenie Odwołującego zaoferowane oprogramowanie nie spełnia wymagań określonych przez Zamawiającego w opisie przedmiotu zamówienia. W ofercie nie podano rodzaju licencji, co uniemożliwia wskazanie konkretnego rozwiązania. W ofercie wymieniony jest produkt „Cortex XDR" ale ten produkt nie jest sprzedawany w takiej formie, jest sprzedawany jako Cortex XDR Prevent lub Cortex XDR Pro.

Na podstawie wyróżnienia tych produktów Odwołujący kwestionował spełnienie szczegółowych parametrów stanowiących wymagania dotyczące przedmiotu zamówienia.

Izba oddaliła zarzuty wobec tej oferty przyjmując, jako istotną z punktu widzenia argumentów okoliczność wskazaną w odpowiedzi na odwołanie, o nieaktualności dokumentów dotyczących produktów Cortex XDR Pro o Prevent. Pomimo oczywistej niespójności argumentacji z obecnym stanem, Odwołujący próbował wykazać niezgodność, której podstawa opiera się na wyróżnieniu dwóch produktów, które Wykonawca miał zidentyfikować w ofercie. Zamawiający wskazując na aktualną dokumentację wykazał, iż oprogramowanie Cortex XDR to rozszerzona chmurowa platforma wykrywania zagrożeń posiadająca funkcjonalności całego rozwiązania XDR. Odnoszenie się do szczegółowych parametrów w tych okolicznościach nie miało znaczenia, gdyż w każdym z parametrów należałoby wskazać, iż zarzut opiera się na błędnym założeniu co do istoty rozwiązania XDR.

W świetle powyższego odwołanie w całości podlegało oddaleniu.

Orzekając o kosztach postępowania odwoławczego orzeczono stosownie do wyniku na podstawie art. 575 Ustawy Prawa zamówień publicznych oraz w oparciu o przepisy § 5 ust. 2 w zw. z § 8 ust. 2 pkt 1 oz. 2437).

Izba zaliczyła do kosztów postępowania wpis w wysokości 15.000 zł i obciążyła nimi w całości Odwołującego.

Przewodnicząca: ……..….