Warszawa dnia 9 sierpnia 2019 r.

Strona WWW

WYJAŚNIENIA I ZMIANY SIWZ NR 2

dot. postępowania na dostawę, montaż i konfigurację Programowalnej Sieci Komputerowej (ang. SDN) – COI-ZAK.262.22.2019

Centralny Ośrodek Informatyki, działając jako Zamawiający, w postępowaniu na **dostawę, montaż i konfigurację Programowalnej Sieci Komputerowej (ang. SDN) ,** na podstawie art. 38 ust. 2 i 4 ustawy z dnia 29 stycznia 2004 r. - Prawo zamówień publicznych (t.j. Dz. U. z 2018 r., poz. 1986 ze zm.) – zwanej dalej ustawą Pzp, przedstawia poniżej treść pytań Wykonawców wraz z udzielonymi odpowiedziami:

Pytanie nr 1:

IPU § 8 W związku z wymaganiem Zamawiającego w zakresie świadczenia gwarancyjnego i wsparcia technicznego w stosunku do licencjowanego oprogramowania prosimy o podanie informacji czy w przypadku wystąpienia Awarii w licencjonowanym oprogramowaniu, które mogą zostać usunięte wyłącznie przez producenta (ograniczenia te wynikające z warunków licencyjnych) w takim przypadku postanowienia w zakresie czasów naprawy i kar umownych nie będą miały zastosowania? Wykonawca nie ma prawa dokonać naprawy (np. zmian w kodzie źródłowym) a jedynie przekazać takie zgłoszenie do producenta, który to dokonuje naprawy poprzez aktualizacje (patche itd.) a ich termin wykonania nie jest gwarantowany przez żadnego producenta.

Odpowiedź:

Zamawiający zmienia treść par. 8 ust. 7 IPU nadając mu brzmienie:

„Wykonawca zobowiązuje się do usuwania Awarii w ciągu 24 godzin od momentu dokonania zgłoszenia z zastrzeżeniem, że niniejszy termin nie obowiązuje w zakresie Awarii Oprogramowania, które mogą zostać usunięte wyłącznie przez producenta. W przypadku gdy Awaria Oprogramowania może zostać usunięta wyłącznie przez producenta Wykonawca zawiadomi Zamawiającego o tym fakcie co najmniej w formie dokumentowej na adres e-mail wskazany w §13 ust. 1 pkt 1) Umowy w ciągu 24 godzin od momentu dokonania zgłoszenia Awarii".

Pytanie nr 2:

Pytanie dot. SIWZ_II_pkt 5.5

„Zamawiający wymaga, aby Wykonawca posiadał najwyższy status partnerstwa przyznawany przez producenta oprogramowania i sprzętu potwierdzony poświadczeniem producenta.

Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa w zdaniu poprzednim."

Odpowiedź:

Zamawiający wymaga , aby Wykonawca i jego podwykonawca posiadali status partnerstwa Producenta zaoferowanego oprogramowania i sprzętu.

Zamawiający zmienia wymóg dotyczący najwyższego statusu partnerstwa na:

„Wykonawca powinien posiadać status partnera producenta sprzętu oraz oprogramowania, których wartościowy udział w zamówieniu jest najwyższy (wykaz sprzętu oraz oprogramowania znajduje się w pkt 6 formularza oferty), z zastrzeżeniem, że jeśli producent stosuje kilka poziomów partnerstwa,

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Zamawiający wymaga, aby wykonawca posiadał nie niższy niż drugi w kolejności poziom partnerstwa licząc od najwyższego poziomu partnerstwa w hierarchii poziomów partnerstwa stosowanej przez producenta. Zamawiający wyklucza, aby wyłącznie podwykonawca posiadał status, o którym mowa jest w zdaniu poprzedzającym."

Pytanie nr 3:

Oferty wykonawców mogą bazować na rozwiązaniach kilku producentów, jednakże udział procentowy niektórych z nich może być znacząco mniejszy od udziału procentowego technologii wiodącej w całym projekcie, a posiadanie najwyższych certyfikatów producentów dla wszystkich zaproponowanych w ofercie produktów może znacząco ograniczyć konkurencyjność oferentów.
Czy zatem powyższe wymaganie z SIWZ należy interpretować jako wymóg w odniesieniu do technologii wiodącej (sprzęt i oprogramowanie), którą oferent proponuje?

Odpowiedź:

Odpowiedzi udzielono w Pytaniu nr 2.

Pytanie nr 4:

§ 4 ust. 1 pkt. 10 - wymóg posiadania przez cały okres obowiązywania Umowy najwyższego statusu partnerstwa przyznawanego przez producenta oprogramowania i sprzętu potwierdzonego poświadczeniem producenta.
Wymóg taki jest nadmiarowy, status partnerstwa nie jest uzależniony wyłącznie (i nie głównie) od posiadanych kompetencji i to w obszarze przedmiotu zamówienia, natomiast jest uzależniony od wielkości zakupów, w tym niezwiązanych z przedmiotem zamówienia (np. nie dotyczących sprzętu sieciowego). Czy Zamawiający wyrazi zgodę na usunięcie pkt. 10.

Odpowiedź:

Odpowiedzi udzielono w Pytaniu nr 2.

Pytanie nr 5:

Jak sama nazwa postępowania wskazuje Zamawiający oczekuje dostarczenia i konfiguracji programowej sieci komputerowej.
Prosimy o rozdzielenie w postępowaniu na min. 2 zadania (osobno oceniane) warstwy sprzętowej od warstwy oprogramowania ponieważ tylko w takiej konfiguracji Zamawiający otrzyma Programowalną Sieć Komputerową (SDN). Przy obecnej formie zapytania postepowanie zakłada wdrożenie dostawy urządzeń sieciowy wraz z oprogramowanie do zarządzania i monitoringu.

Odpowiedź:

Zamawiający nie wyraża zgody na zmianę SIWZ.
Zamawiający wymaga dostawy kompletnego rozwiązania SDN składającego się z urządzeń sieciowych, oprogramowania oraz kontrolera. Obowiązkiem oferującego rozwiązanie jest dostarczenie wszystkich niezbędnych komponentów wybranych producentów, wzajemna integracja i konfiguracja do uruchomienia gotowego środowiska programowalnej sieci SDN. Przedmiotem zamówienia nie jest dostawa urządzeń i oprogramowania, które samodzielnie będą spełniać konkretne wymagania, ale dostawa tak dobranych urządzeń i oprogramowania, które będą ze sobą kompatybilne i będą po wdrożeniu i skonfigurowaniu łącznie ze sobą współpracować, zapewniając funkcjonalności określone przez Zamawiającego. Obowiązkiem Wykonawcy jest więc zapoznanie się z wymaganiami Zamawiającego dotyczącymi infrastruktury, z którą kompatybilne musi być dostarczane rozwiązanie, i

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

zaproponowanie takich urządzeń wraz z oprogramowaniem, które stworzą spójny, bezawaryjny system.

Pytanie nr 6:

Zamawiający w Kryteriach oceny jako najwyżej oceniane kryterium (23.6.2) zdefiniował Unifikację środowiska sprzętowego. Takie kryterium przy zakupie Programowalnej Sieci Komputerowej znacząco ogranicza konkurencyjność postępowania i naraża Zamawiającego na znacząco wyższe koszty zarówno zakupu (firmy sprzętowe zawyżą swoją cenę) jak i późniejszych rozbudów (firma sprzętowa będzie sprzedawała do Zamawiającego przełączniki w cenie „katalogowej" bo tylko takie będą wspierane przez SDN).

Celem zwiększenia konkurencyjności postępowania i zabezpieczenia interesu Zamawiającego prosimy o zmianę tego kryterium oceny na Kryterium premiujące dostawców Programowalnej Sieci Komputerowej współpracującej z min. 2 producentami sprzętu.

Odpowiedź:

Zamawiający pragnie zwrócić uwagę, że kryterium pod nazwą „unifikacja środowiska sprzętowego" pozwala na otrzymanie dodatkowych punktów za zaoferowanie jednolitego środowiska programowo –sprzętowego. Tym samym za zgodne z SIWZ zostanie uznane niejednolite środowisko programowo-sprzętowe z zastrzeżeniem, że Wykonawca takiego rozwiązania nie otrzyma dodatkowych punktów w ramach wspomnianego kryterium oceny ofert. W związku z tym Zamawiający nie ograniczył konkurencji w niniejszym postępowaniu a parametry zawarte w OPZ mogą zostać spełnione również przez Wykonawcę, który dostarczy niejednolite środowisko programowo-sprzętowe.

Celem zastosowania kryterium unifikacji środowiska programowo - sprzętowego, jest zmniejszenie kosztów utrzymania i zarządzania infrastrukturą oraz ułatwienie rozwiązywania problemów technicznych i ewentualnych awarii. Stanowi także ułatwienie dla pracowników Zamawiającego w zarządzaniu środowiskiem. Zamawiający dopuszcza implementację wykorzystującą sprzęt oraz oprogramowanie różnych producentów, pod warunkiem ich integracji w ramach programowalnej platformy SDN. Biorąc pod uwagę, powyższe argumenty, Zamawiający nie wyraża zgody na zmianę SIWZ.

Pytanie nr 7:

W środowiskach czołowych producentów SDN polityki filtrowania mogą być zarządzane z jednego widoku, jak w innych firewallach. Takie podejście jest faktycznym ułatwieniem w zarządzaniu. Prosimy o rozważenie wprowadzenie takiego wymagania oraz wykluczenia Kryterium oceny Unifikacja środowiska sprzętowego" (US), które to zawęża producentów SDN jedynie do firmy Cisco.

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania, w którym polityki filtrowania konfigurowane są z poziomu kontrolera SDN. W zakresie pytania dotyczącego unifikacji zgodnie z odpowiedzią na pytanie nr 6.

Pytanie nr 8:

W celu złożenia oferty pod względem licencyjnym prosimy o podanie podziału ilościowego dla 2000 VM i 500 serwerów fizycznych na poszczególne wirtualizatory i serwery fizyczne:

Hyper-V

VMware vSphere

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

KVM
Serwery fizyczne bez wirtualizatorów
Serwery fizyczne z platformą kontenerową wraz z nazwą systemu do zarządzania kontenerami.
Definicja ilości portów wskazuje na model licencjonowania Cisco i uniemożliwia optymalne dobranie licencji w oparciu o produkty SDN czołowych dostawców.

Odpowiedź:

Zamawiający wskazuje, że w OPZ nie narzucił szczegółowych modeli licencjonowania. Zamawiający wymaga natomiast, aby całe dostarczone środowisko programowo – sprzętowe zostało prawidłowo zalicencjonowane.
Informacja o ilości serwerów fizycznych została podana w OPZ. Nie specyfikuje w żaden sposób dostawcy rozwiązania SDN ani modelu licencjonowania. W OPZ Zamawiający nie zawarł definicji „ilości portów" a jedynie określił w OPZ wymagane ilości portów dla urządzeń fizycznych co jest jednym z podstawowych parametrów technicznych urządzenia sieciowego oferowanego przez każdego producenta, a nie tylko wskazanego w pytaniu.

Pytanie nr 9:

Zamawiający wymaga dostarczenia rozwiązania klasy SDN z funkcjonalnościami bezpieczeństwa, ale nie oczekuje ani nie punktuje dodatkowo w kryteriach oceny dostawy produktu spełanijącego rekomendacje z zakresu bezpieczeństwa. Prosimy o rozważenie dodania kryterium oceny lub wymagania spełnienia rekomendacji zgodnych z dyrektywą NIST.SP.800-125B.

Odpowiedź:

Zgodnie z najlepszą wiedzą Zamawiającego, Dyrektywa NIST nie stanowi ciała certyfikującego rozwiązania bezpieczeństwa na terenie Polski lub krajów Unii Europejskiej. Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający nie organicza rozwiązania spełniającego wspomnianą rekomendację. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 10:

Zamawiający w wymaganiach oczekuje rozwiązania pracującego w oparciu o Protokół COOP. Natomiast COOP jest protokołem wprowadzonym przez Cisco i wykorzystuje go tylko firma CISCO w implementacji SDN w formie ACI. Prosimy o usuniecie z SIWZ wymagań wskazujących jedynie na jednego dostawcę tzn.:

a. Kryterium oceny 23.6.2
b. Wymagań: 8.4.6.3, 8.4.6.7 oraz 8.4.6.8.
c. Wymagania dostawy przełączników IPN

Odpowiedź:

Zamawiający wskazuje, że w OPZ nie zawarł (nawet pośrednio) wymogu aby dostarczane rozwiązanie pracowało w oparciu o protokół COOP. Należy podkreślić, że rozwiązanie każdego producenta pracuje w oparciu inny protokół. Tym samym Zamawiający dopuszcza zastosowanie różnych protokołów. Według najlepszej wiedzy Zamawiającego, wskazane przez Wykonawcę w pytaniu wymagania techniczne nie dotyczą funkcjonalności, które są realizowane poprzez protokół COOP.
Zamawiający wymaga dostawy kompletnego rozwiązania SDN składającego się z urządzeń sieciowych, oprogramowania oraz kontrolera. Obowiązkiem oferującego rozwiązanie jest dostarczenie wszystkich niezbędnych komponentów wybranych producentów, wzajemna integracja i konfiguracja do

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

uruchomienia gotowego środowiska programowalnej sieci SDN. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 11:

Czy oferowany SDN ma być wspierany przez dostawców hypervisorów. Prosimy o podanie jakie technologie wirtualizacji będą objęte SDN w trakcie inicjalnego wdrożenia planowanego na 15 dni.

Odpowiedź:

Zamawiający wyjaśnia, że to producent oferowanego rozwiązania SDN ma wspierać hypervisory, a nie hyrpervisory mają wspierać producenta oferowanego rozwiązania SDN. Lista hypervisorów powinna wynikać z dostarczonej przez Wykonawcę dokumentacji technicznej. W trakcie konfiguracji wymagane będzie wdrożenie testowe wszystkich wymienionych hypervisorów.

Pytanie nr 12:

Prosimy o informacje dlaczego Zamawiający nie wymaga dostarczenia rozwiązania SDN niezależnego od matrycy przełączającej (od sprzętu). Oszczędności i elastyczność SDN zaczyna się w momencie kiedy następuje unifikacja od sprzętu. Powstaje pytanie czy Zamawiający chce kupić sprzęt sieciowy czy rozwiązanie Sieci Programowalnej? Bazując na rekomendacjach niezależnych organizacji sugerujemy rozdział warstwy sprzętowej od warstwy SDN.

Odpowiedź:

Zamawiający wymaga dostawy kompletnego rozwiązania SDN składającego się z urządzeń sieciowych, oprogramowania oraz kontrolera. Obowiązkiem oferującego rozwiązanie jest dostarczenie wszystkich niezbędnych komponentów wybranych producentów, wzajemna integracja i konfiguracja do uruchomienia gotowego środowiska programowalnej sieci SDN. Przedmiotem zamówienia nie jest dostawa urządzeń i oprogramowania, które samodzielnie będą spełniać konkretne wymagania, ale dostawa tak dobranych urządzeń i oprogramowania, które będą ze sobą kompatybilne i będą po wdrożeniu i skonfigurowaniu łącznie ze sobą współpracować, zapewniając funkcjonalności określone przez Zamawiającego. Obowiązkiem Wykonawcy jest więc zapoznanie się z wymaganiami Zamawiającego dotyczącymi infrastruktury, z którą kompatybilne musi być dostarczane rozwiązanie, i zaproponowanie takich urządzeń wraz z oprogramowaniem, które stworzą spójny, bezawaryjny system.

Pytanie nr 13:

Dotyczy wymagania: „9.6.1. przepustowość szyfrowania (sprzętowa) minimum 18Gbps, 15000 TPS (algorytm oparty o krzywe eliptyczne z kluczem 256bit); 9.6.2. przepustowość minimum 40Gbps L4/L7;"

Biorąc pod uwagę fakt, że aktualnie większość ruchu HTTP jest szyfrowana, wydaje się że ponad dwukrotna rozbieżność wydajności load-balancera dla ruchu nieszyfrowanego i szyfrowanego nie jest uzasadniona.

Czy w takim razie Zamawiający zaakceptuje urządzenie o wydajności minimum 18Gbps zarówno dla ruchu szyfrowanego jak i nieszyfrowanego? Ewentualnie, jeśli Zamawiający przewiduje ruch na poziomie 40Gbps, sugerujemy podniesienie wymagania na wydajność dla ruchu szyfrowanego również do 40Gbps.

Czy Zamawiający podnosi wymagania na wydajność ruchu szyfrowanego do 40Gbps?

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Odpowiedź:
Zamawiający wyjaśnia, że wymagana przepustowość wynika z potrzeb Zamawiającego poprzedzonych analizą techniczną i wobec tego potwierdza, że wymaganie jest celowe. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 14:
Dotyczy wymagania: „9.6.10. minimum 4 porty 10GBASE-SR;" W związku z tym, że planowana infrastruktura sieciowa składać się będzie w większości z przełączników wyposażonych w porty 25G chcielibyśmy się upewnić, czy to wymaganie nie jest omyłką i czy Zamawiający nie oczekuje load-balancerów wyposażonych w porty o szybkości co najmniej 25Gbit, co pozwoliłyby w pełni optymalnie wykorzystać nową infrastrukturę sieciową?
Odpowiedź:
Zamawiający wyjaśnia, że wymagana prędkość portu wynika z potrzeb Zamawiającego poprzedzonych analizą techniczną i wobec tego potwierdza, że wymaganie jest celowe. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 15:
Dotyczy wymagania: 9.6.14. posiada możliwość kreowania minimum 5 partycji wirtualnych (osobne tablice routingu);
Prosimy o doprecyzowanie, czy przez partycje wirtualne Zamawiający rozumie jedynie osobne tablice routingu, czy też możliwość uruchomienia na urządzeniu fizycznym co najmniej 5 niezależnych wirtualnych instancji urządzenia? Gdzie każda z tych instancji może pracować na innej wersji oprogramowania, mieć dedykowane dla siebie zasoby sprzętowe (CPU, RAM, HDD) oraz interfejsy sieciowe czy pasmo.
Odpowiedź:
Odpowiedź została udzielona do pytania nr 16 z dnia 2 sierpnia 2019 r.

Pytanie nr 16:
Zamawiający w pkt. 8.1.1. („**Centralnego kontrolera SDN** zarządzającego siecią fizyczną, wirtualną, kontenerową oraz warstwą logiczną i zapewniającego uruchamianie usług w oparciu o modelowanie polityk dla aplikacji;") wymaga, aby rozwiązanie posiadało rozwiązanie typu SDN i zarządzało siecią kontenerową. Jednak w dalszej części dokumentu nie ma dokładnej specyfikacji, jak ma być, to obsługiwane.
Punkt 8.4.6.6 wymienia wsparcie platformy dla środowisk kontenerowych, natomiast specyfikacja kontrolera SDN nie wspomina o wymaganiach odnośnie wsparcia takiej platformy. Jak system analizy aplikacji ma kontrolować środowisko kontenerowe, skoro kontroler SDN nie ma wymagań odnośnie takiego środowiska?
W tym momencie najbardziej popularną technologią na świecie do zarządzania kontenerami jest platforma Kubernetes.
W związku z tym, czy docelowe rozwiązanie SDN, nie musi chociaż w minimalnym stopniu zarządzać siecią platformy Kubernetes, która może być zbudowana na serwerach fizycznych lub/i serwerach wirtualnych?
Należy zauważyć, że świat sieci kontenerowych Kubernetes, jest dla tradycyjnego administratora sieci i bezpieczeństwa czarną skrzynką. Dlatego rozwiązanie powinno mieć narzędzia ułatwiające prace administracyjne w tym obszarze.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Dlatego sugerujemy dla platformy Kubernetes, aby proponowane rozwiązanie SDN wspierało:

1. Load Balancer, NAT oraz IPAM zintegrowany z siecią kontenerów?
2. Izolowanie i filtrowanie ruchu pomiędzy podami kontenerów K8S. Filtrowanie na bazie tagów (niezależność od fizycznej adresacji).
3. Monitorowanie przepływów i rozwiązywanie problemów sieciowych ruchu wewnątrz klastra oraz workera Kubernetesa."

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 17:

Zamawiający wymaga w pkt. 9.2.8.8, 9.3.8.8, 9.4.8.8 zastosowania technologii do obsługi logów – Syslog. Biorąc pod uwagę, tak złożone rozwiązanie z wieloma punktami powstawania logów naturalnym staje się posiadanie narzędzia do zbierania logów, a następnie ich korelacji, graficznej interpretacji, agregowania tych samych zdarzeń w celu szybkiego przeszykowania logów, które wywołały awarię. Dodatkowo, takie narzędzie powinno mieć możliwości zbierania logów pochodzących z Access List (czy dana polityka bezpieczeństwa jest skuteczna). Z doświadczeń naszych oraz naszych klientów wynika, iż tylko tego typu rozwiązanie przekłada się na skuteczność, niezawodność i szybkość rozwiązywania problemów w infrastrukturze.
Czy dostarczone rozwiązanie powinno zapewniać opisane powyżej funkcjonalności?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 18:

Ilości portów oraz wielkość zamówienia sugeruje, że rozwiązanie docelowo, będzie zarządzało dużą ilością infrastruktury zwirtualizowanej oraz fizycznej. Przy tego typu inwestycji, która ma działać przez kolejne 5 lat, należy spodziewać się pojawienia elementów portalu samoobsługowego, gdzie klienci będą mogli samodzielnie zamawiać infrastrukturę w modelu IaaS. Czy zamawiane rozwiązanie SDN powinno dawać możliwość:

1. swobodnego, bezpiecznego, bez zmiany ustawień adresacji IP oraz mikrosegmentacji migracji workload w czasie rzeczywistym pomiędzy infrastrukturą lokalną, a chmurami publicznymi (np. AWS, polskie firmy: Beyond, OCHK)?
2. Integracji z graficznymi narzędziami do tworzenia usług IaaS dla klientów w oparciu o elementy infrastruktury sieciowej SDN tj. LB, Routing, FW, NAT, itp. (bez dodatkowej pracy programistycznej/skryptowej)?

Odpowiedź:

Zamawiający informuje, że dostarczenie takiego portalu nie jest wymagane w ramach postępowania. Wymagane jest natomiast, aby platforma SDN posiadała otwarte interfejsy programistyczne celem ewentualnej, przyszłej integracji z dostępnymi na rynku rozwiązaniami. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 | Fax: 22 250 29 87 | coi@coi.gov.pl | www.coi.gov.pl

Pytanie nr 19:

Dotyczy monitorowania maszyn wirtualnych. Czy rozwiązanie powinno posiadać możliwości bezagentowego monitorowania, izolowania VM pod kątem zagrożeń malware/virus na warstwie innej niż system operacyjny maszyny wirtualnej?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 20:

Zgodnie z przyjętymi rekomendacjami bezpieczeństwa przez Unię Europejską w ramach "ICT Standards for Procurement" dla aplikacji wrażliwych na opóźnienia oraz intensywnie przetwarzające dane wejściowo-wyjściowe zaleca się zastosowanie wirtualnych firewalli działających bezpośrednio jako moduł w kernelu na platformach wirtualnych. Źródło: https://joinup.ec.europa.eu/solution/nist-special-publication-800-125-guide-security-full-virtualization-technologies/distribution/nist-special-publication-800-125-guide-security-full-virtualization-technologies

Czy zamawiający posiada taką grupę aplikacji, która wymagałaby ścisłej ochrony firewalla stanowego L3-L7 na serwerach bez konieczności zawijania ruchu na przełączniku typu Leaf, gdzie ma być wyłącznie filtrowanie bezstanowe L3-L4? Jeżeli jest taka grupa wrażliwych aplikacji, to czy zamawiający zgadza się na wyspecyfikowanie liczby serwerów, na których aplikacje będą chronione za pomocą wirtualnego firewalla L3-L7, który będzie zainstalowany bezpośrednio jako moduł hyperwizora i chronił aplikacje w ramach hosta?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 21:

Dotyczy wymagania 8.4.2.4.

Zgodnie z obowiązującymi praktykami możliwe jest zastosowanie rozwiązania bezagentowego. Czy zamawiający dopuszcza takie rozwiązanie?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 22:

Dotyczy wymagania 8.4.6.3.

Z punktu widzenia wymagań sieci SDN w tym postępowaniu kluczowe jest sterowanie ruchem i zarządzanie bezpieczeństwem na poziomie aplikacji. Czy zamawiający dopuszcza funkcjonalność wizualizacji realizowaną na poziomie aplikacji, a nie na poziomie procesów?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Pytanie nr 23:

Dotyczy wymagania 8.4.6.4.

Zgodnie z obowiązującymi praktykami możliwe jest zastosowanie rozwiązania bezagentowego. Czy zamawiający dopuszcza takie rozwiązanie?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 24:

Dotyczy wymagania 8.4.6.7.

Bazy CVE są powszechnie dostępne i darmowe. Dodatkowo istnieją dedykowane rozwiązania, typu skanery podatności które pozwalają na zidentyfikowanie, jakie konkretne podatności mogą dotyczyć danych stacji końcowych. Najlepsza praktyka bezpieczeństwa rekomenduje stosowanie rozwiązań do wyszukiwania podatności oraz ochrony przed nimi pochodzących od różnych dostawców. Sugerujemy zamawiającemu zastosowanie zewnętrznych i dedykowanych systemów typu skanery podatności do realizowania tej funkcjonalności. Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego punktu OPZ?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 25:

Dotyczy wymagania 8.4.6.8.

Analogicznie jak dla punktu 8.4.6.7, Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego punktu OPZ?

Odpowiedź:

Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 26:

Dotyczy wymagania 8.4.6.9.

Zgodnie z obowiązującymi praktykami bezpieczeństwa i zwiększonym ryzykiem podatności na złośliwy malware w ramach tego samego systemu operacyjnego realizacja procesu wymuszania polityki bezpieczeństwa powinna odbywać się poza systemem operacyjnym. Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego punktu OPZ?

Odpowiedź:

Zamawiający nie wyklucza zastosowania takiego rozwiązania nie mniej jednak nie stanowi ono obowiązkowej funkcjonalności zawartej w OPZ. Zamawiający podkreśla, że dopuszcza zastosowanie rozwiązania w zakresie wskazanym w pytaniu. Zamawiający utrzymuje zapisy SIWZ w tym zakresie.

Pytanie nr 27:

Zgodnie z przyjętymi rekomendacjami bezpieczeństwa przez Unię Europejską w ramach "ICT Standards for Procurement" dla aplikacji wrażliwych na opóźnienia oraz intensywnie przetwarzające dane

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

wejściowo-wyjściowe zaleca się zastosowanie wirtualnych firewalli działających bezpośrednio jako moduł w kernelu na platformach wirtualnych. Źródło: https://joinup.ec.europa.eu/solution/nist-special-publication-800-125-guide-security-full-virtualization-technologies/distribution/nist-special-publication-800-125-guide-security-full-virtualization-technologies
Czy zamawiający posiada taką grupę aplikacji, która wymagałaby ścisłej ochrony firewalla stanowego L3-L7 na serwerach bez konieczności zawijania ruchu na przełączniku typu Leaf, gdzie ma być wyłącznie filtrowanie bezstanowe L3-L4? Jeżeli jest taka grupa wrażliwych aplikacji, to czy zamawiający zgadza się na wyspecyfikowanie liczby serwerów na których aplikacje będą chronione za pomocą wirtualnego firewalla L3-L7, który będzie zainstalowany bezpośrednio jako moduł hyperwizora i chronił aplikacje w ramach hosta ?

Odpowiedź:

Odpowiedzi udzielono w pytaniu nr 20.

Pytanie nr 28:

Dotyczy 8.4.2.4

Zgodnie z obowiązującymi praktykami możliwe jest zastosowanie rozwiązania bezagentowego. Czy zamawiający dopuszcza takie rozwiązanie?

Odpowiedź:

Odpowiedzi udzielono w pytaniu nr 21.

Pytanie nr 29:

Dotyczy 8.4.6.3

Z punktu widzenia wymagań sieci SDN w tym postępowaniu kluczowe jest sterowanie ruchem i zarządzanie bezpieczeństwem na poziomie aplikacji. Czy zamawiający dopuszcza funkcjonalność wizualizacji realizowaną na poziomie aplikacji a nie na poziomie procesów ?

Odpowiedź:

Odpowiedzi udzielono w pytaniu nr 22.

Pytanie nr 30:

Dotyczy 8.4.6.4

Zgodnie z obowiązującymi praktykami możliwe jest zastosowanie rozwiązania bezagentowego. Czy zamawiający dopuszcza takie rozwiązanie?

Odpowiedź:

Odpowiedzi udzielono w pytaniu nr 23.

Pytanie nr 31:

Dotyczy 8.4.6.7

Bazy CVE są powszechnie dostępne i darmowe. Dodatkowo istnieją dedykowane rozwiązania, typu skanery podatności które pozwalają na zidentyfikowanie jakie konkretne podatności mogą dotyczyć danych stacji końcowych. Najlepsza praktyka bezpieczeństwa rekomenduje stosowanie rozwiązań do wyszukiwania podatności oraz ochrony przed nimi pochodzących od różnych dostawców. Sugerujemy zamawiającemu zastosowanie zewnętrznych i dedykowanych systemów typu skanery podatności do realizowania tej funkcjonalności. Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego zapisu?

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

Odpowiedź:
Odpowiedzi udzielono w pytaniu nr 24.

Pytanie nr 32:
Dotyczy 8.4.6.8
Analogicznie jak dla punktu 8.4.6.7, Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego zapisu?
Odpowiedź:
Odpowiedzi udzielono w pytaniu nr 25.

Pytanie nr 33:
Dotyczy 8.4.6.9
Zgodnie z obowiązującymi praktykami bezpieczeństwa i zwiększonym ryzykiem podatności na złośliwy malware w ramach tego samego systemu operacyjnego realizacja procesu wymuszania polityki bezpieczeństwa powinna odbywać się poza systemem operacyjnym. Czy zamawiający w zgodzie z obowiązującymi rekomendacjami dopuszcza usunięcie tego zapisu?
Odpowiedź:
Odpowiedzi udzielono w pytaniu nr 26.

Pytanie nr 34:
Z uwagi na brak odpowiedzi na przesłane do Państwa pytania w przedmiotowym postępowaniu oraz zbliżający się termin składania ofert proszę o przesuniecie terminu składania postępowania na termin nie wcześniejszy niż 22.08.2019r. Opublikowane w dniu 2.08.2019r odpowiedzi nie zmieniają w znaczący sposób wymagań technicznych co powoduje konieczność zastosowania dodatkowych komponentów i rozwiązań technologicznych, a więc czas przygotowania ofert konkurencyjnych do rozwiązania CISCO się wydłuża. Dodatkowo w tygodniu roboczym 12-16.08 mamy dzień świąteczny a co za tym idzie praca nad przygotowaniem ofert będzie utrudniona w podmiotach polskich (firmy integratorskie oraz dystrybucyjne).
Dodatkowo proszę o podanie jaka ilość serwerów będzie objęta usługą wdrożenia dostarczaną przez Oferentów. Dodatkowo proszę o podanie ich konfiguracji (ilość CPU, ilość core na CPU, ilość RAM, system operacyjny, ilość instancji maszyn wirtualnych)
Odpowiedź:
Zamawiający wyjaśnia, że wdrożenie obejmuje środowisko programowo-sprzętowe dostarczone przez Wykonawcę. Przedmiotem wdrożenia nie będzie migracja infrastruktury posiadanej przez Zamawiającego. Zakres prac został określony w odpowiedzi na pytanie nr 17 z dnia 2 sierpnia 2019 r.

Ponadto Zamawiający informuje, że na podstawie art. 38 ust. 4 ustawy Pzp przedłuża termin składania ofert do dnia 22/08/2019 r. do godz. 11:00.
Odpowiednio zmianie ulegają zapisy w rozdziale I SIWZ:

1) ust. 18.1. otrzymuje brzmienie:
   Ofertę należy złożyć za pośrednictwem formularza do złożenia, zmiany, wycofania oferty lub wniosku dostępnego na ePUAP i udostępnionego również na miniPortalu w nieprzekraczalnym terminie:

do dnia	**22/08/2019 r.**	do godz.	**11:00**

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl

2) ust. 18.3. otrzymuje brzmienie:

Otwarcie ofert nastąpi w siedzibie **Centralnego Ośrodka Informatyki, Aleje Jerozolimskie 132-136, 02-305 Warszawa, sala konferencyjna**.

W dniu	**22/08/2019 r.**	o godz.	**13:00**

Niniejsze wyjaśnienia i zmiany stanowią integralną część SIWZ.

Dyrektor
Centralnego Ośrodka Informatyki
Marcin Walentynowicz
09.08.2019 r.

Kierownik Zespołu Zakupów
Magdalena Jagielska

Dyrektor
Pionu Operacji
Sebastian Bukowski

Radca Prawny
Stanisław Chajewski

Aleje Jerozolimskie 132 - 136, 02- 305 Warszawa Tel.: 22 250 28 83 I Fax: 22 250 29 87 I coi@coi.gov.pl I www.coi.gov.pl