Punkt 3.2 OPZ

W OPZ do postępowania widnieje zapis "Wykonawca musi posiadać kapitał zakładowy przynajmniej na poziomie wartości Usługi"

Czy istnieje możliwość zniesienia tego warunku dla wykonawców chcących przystąpić do postępowania?

Zamawiający nie wyraża zgody na zniesienie tego warunku.

Punkt 3.7 OPZ

Wykonawca zapewni obsługę minimum 500 EPS (events per second).

Czy Zamawiający może doprecyzować maksymalną ilość obsługiwanych EPS (events per second) oraz czy zwiększanie ich powyżej minimum będzie skutkowało aneksowaniem istniejącej umowy?

Zamawiający określa minimalną ilość obsługiwanych zdarzeń. Pojawienie się większej niż podana ilość zdarzeń nie będzie skutkowało aneksowaniem zawartej umowy. Zamawiający nie jest w stanie doprecyzować maksymalnej ilości obsługiwanych EPS.

Punkt 3.10 OPZ

Czy Zamawiający dopuszcza obsługę do 10 alarmów dziennie na poziomie krytycznym i średnim?

Zamawiający dopuszcza obsługę do 10 alarmów krytycznych dziennie w trybie określonym w SLA w punkcie 3.10 OPZ. Pozostałe incydenty obsługiwane w trybie best effort.

Punkt 4.1.1.5 OPZ

Czy Zamawiający może doprecyzować zakres takiego skanowania, posiada gotowy „Asset management", źródła informacji, zasoby jakie podlegałby skanowaniu?

Poprzez skanowanie systemów i usług Zamawiający rozumie działania zmierzające w kierunku znalezienia podatności oraz błędów w konfiguracji urządzeń w celu zaplanowania działań ograniczających możliwość włamania i wycieku danych z systemów Zamawiającego.

Punkt 4.1.1.5 OPZ

Jakiego poziomu skanowania podatności wymaga Zamawiający z poświadczeniami czy bez?

Zamawiający oczekuje skanowania bez znajomości/wykorzystania poświadczeń użytkowników systemu.

Punkt 4.1.1.5 OPZ

Czy Zamawiający jest w posiadaniu licencji lub narzędzia do skanowania czy będzie ono w całości w gestii Wykonawcy?

Przeprowadzanie skanowanie będzie w całości po stronie Wykonawcy

Punkt 4.1.1.5 OPZ

Czy Zamawiający oczekuje wstawienia skanera podatności bezpośrednio w infrastrukturę Zamawiającego i jest w stanie wygospodarować maszynę fizyczną lub wirtualne zasoby na takie potrzeby?

Zamawiający jest w stanie wygospodarować zasoby wirtualne na potrzeby skanera podatności.

Punkt 4.1.1.5 OPZ

Czy dla Zamawiającego wystarczającym będzie skanowanie podatności cyklicznie raz na kwartał zakończone raportem

Cykliczne skanowanie podatności raz na kwartał zakończone raportem będzie wystarczające. Zamawiający przewiduje możliwość dodatkowego przeprowadzenia skanowania podatności w przypadku znaczącej zmiany architektury i elementów systemu Zamawiającego lub wykrycia nowej podatności w skanowanych systemach.

Punkt 4.1.1.5 OPZ

Jakiego typu i ile szacunkowo urządzeń infrastruktury klienta ma podlegać skanowaniu pod względem podatności (np.: Window/Linux/… 100/1000/10k)?

Zamawiający w swojej infrastrukturze posiada serwery oraz domenę MS Windows, serwery MS Exchange, stacje robocze pracujące po kontrolą systemu MS Windows, switche, routery, firewall, system bezpiecznego dostępu do sieci, bramę e-mail. Zamawiający nie jest aktualnie w stanie określić jaka ilość poszczególnych elementów systemu powinna być objęta skanowaniem. W zakresie wyboru optymalnego rozwiązania Zamawiający polega na wiedzy i doświadczeniu Wykonawcy, który po zapoznaniu się z architekturą systemu Zamawiającego powinien zaproponować optymalne rozwiązanie.

Punkt 4.1.1.5 OPZ

Czy Zamawiający posiada istniejący proces wewnętrzny i cykliczny wgrywania patchy na swoją infrastrukturę?

Zamawiający posiada wewnętrzny proces aktualizacji posiadanych systemów.

Punkt 4.1.2.2 OPZ

Czy dobrze rozumiemy że w ramach troubleshooting Zamawiający oczekuje identyfikacji i rozwiązywania problemów związanych z działaniem systemu SIEM?

W ramach troubleshooting Zamawiający oczekuje propozycji działań zmierzających do likwidacji podatności wykrytych w ramach świadczenia usługi w systemach podlegających monitorowaniu.

Punkt 4.1.2.3 OPZ

Czy dobrze rozumiemy, że w ramach strojenia systemów Zamawiający wymaga integracji rozwiązania SIEM dostarczonego przez Wykonawcę z istniejącą infrastrukturą Zamawiającego, wspólnie z administratorami systemów oraz podłączenie niezbędnych źródeł wymaganych do realizacji scenariuszy bezpieczeństwa?

Zamawiający wymaga integracji systemu SIEM Wykonawcy z elementami systemu Zamawiającego podlegającymi monitorowaniu w celu prawidłowej interpretacji i korelacji otrzymywanych logów oraz eliminację alertów false positive.

Punkt 4.1.2.4 OPZ

Czy Zamawiający ma na myśli propozycję uzgodnionych z Zamawiającym minimum 10 scenariuszy reagowania na wykryte incydenty?

Zamawiający ma na myśli tworzenie nowych scenariuszy postępowania z nowymi wykrytymi incydentami dla 1. Linii wsparcia przez specjalistów z 2. Linii wsparcia w czasie realizacji umowy.

Punkt 4.1.2.5 OPZ

Czy Zamawiający może doprecyzować różnice pomiędzy skanowaniem podatności opisanej w L1 w stosunku do wymagania zaawansowanego skanowania w L2

Skanowanie wykonywane przez 1. Linię wsparcia dotyczy skanowania automatycznego. Skanowanie wykonywane przez 2. Linię wsparcia w przypadku wykrycia nowych podatności przez 1. Linię wsparcia obejmuje ewentualne dokładne skanowanie w kierunku wykrytej podatności oraz komentarz i zalecenia w kierunku obsługi wykrytej podatności.

Punkt 4.1.3.1 OPZ

Czy Zamawiający może doprecyzować jaką ilość złożonych incydentów prognozuje w czasie trwania umowy?

Zamawiający nie jest w stanie określić na etapie postępowania ilości złożonych incydentów w czasie trwania umowy.

Punkt 4.1.3.1 OPZ

Czy Zamawiający może doprecyzować ilość analiz malware przewidzianych w czasie trwania umowy?

Zamawiający nie jest w stanie określić na etapie postępowania ilości analiz malware w czasie trwania umowy.

Punkt 4.1.3.1 OPZ

Czy w ramach analizy malware wystarczającym będzie detonacja w bezpiecznym środowisku wraz z przekazaniem raportu z wykonanej analizy?

Zamawiający uznaje detonację malware w bezpiecznym środowisku (sandbox) wraz z przekazaniem raportu z analizy za wystarczające.

Punkt 4.1.3.1 OPZ

Czy Zamawiający potwierdza, że Wykonawca otrzyma od Zamawiającego próbkę malware do analizy?

W przypadku konieczności wykonania analizy Wykonawca otrzyma próbkę malware do analizy.

Punkt 4.1.3.1 OPZ

Czy Zamawiający może określić jaki typ źródeł danych jest oczekiwany (komputery, komputery przenośne, serwery, telefony (ios/android), systemy przemysłowe, alarmy, chmura?)

Źródłami danych dla systemu Wykonawcy powinny być serwery Microsoft Windows, domena Microsoft Windows, switche, routery, systemy bezpiecznego dostępu do sieci, brama e-mail, firewall, system antywirusowy. Zamawiający polega na wiedzy i doświadczeniu Wykonawcy w kwestii ustalenia źródeł danych poddawanych analizie w celu znalezienia optymalnego rozwiązania.

Punkt 4.1.3.1 OPZ

Czy Zamawiający dopuszcza zabezpieczenie danych robione zdalnie? Jeżeli nie, to czy Zamawiający zakłada ewentualne wysłanie sprzętu do siedziby Wykonawcy? Czy Wykonawca powinien wysłać osobę do wizyty on-site w celu zabezpieczenia sprzętu?

Sposób podejmowania przez 3. Linię wsparcia (L3) działań w przypadku wykrycia incydentu mającego wielowymiarowe konsekwencje lub skutkujące wyciekiem danych będzie indywidualnie uzgadniany

w czasie prowadzenia działań z zakresu informatyki śledczej. Zamawiający dopuszcza wszystkie podane możliwości zabezpieczenia danych skuteczne i adekwatne do wagi analizowanego incydentu.

Punkt 4.1.3.1 OPZ

Jak długo Wykonawca powinien przechowywać fizyczne nośniki?

Zabezpieczone w konsekwencji wykrycia incydentu nośniki danych powinny być przechowywane do momentu zakończenia działań z zakresu informatyki śledczej dotyczącej incydentu przez 3. Linię wsparcia (L3) Wykonawcy oraz inne organy uprawnione do przeprowadzania działań w zakresie incydentu i jego skutków (Policja, Prokuratura, itp.) lub do chwili ich przekazania jako dowód w sprawie uprawnionym organom prowadzącym takie działania.

Punkt 4.1.3.1 OPZ

Czy Wykonawca musi przechowywać wirtualne kopie? Jeżeli tak to jak długo?

Według wiedzy Zamawiającego wirtualne kopie nośników danych powinny być tworzone na potrzeby i na czas wykonywania działań 3. Linii wsparcia w zakresie przeprowadzanej analizy śledczej lub powłamaniowej. Wykonawca dysponując szerszą wiedzą i większym doświadczeniem powinien zaproponować właściwy dla obsługiwanego incydentu czas przechowywania kopii.

Punkt 4.1.3.1 OPZ

Czy Zamawiający może doprecyzować jaką ilość analiz tego typu prognozuje w czasie trwania umowy?

Zamawiający nie jest w stanie określić na etapie postępowania przewidywanej ilości analiz określonych w punkcie 4.1.3.1 OPZ.

Punkt 4.1.3.2 OPZ

Czy Zamawiający może doprecyzować zakres takich testów penetracyjnych, zasoby jakie podlegałby testowaniu i częstotliwość testów?

W ramach możliwości wykorzystania usług 3. Linii wsparcia (L3) Zamawiający oczekuje możliwości przeprowadzenia uzgodnionych z Zamawiającym i bazujących na wiedzy i doświadczeniu Wykonawcy testów penetracyjnych wykorzystujących znane możliwości przeprowadzenia ataku na systemy Zamawiającego, w tym np. ataki socjotechniczne wymierzone w użytkowników systemów Zamawiającego, czy inne metody stosowane współcześnie w atakach na systemy informatyczne.

Punkt 4.1.3.3 OPZ

Czy Zamawiający ma na myśli propozycję uzgodnionych z Zamawiającym minimum 10 scenariuszy reagowania na wykryte incydenty?

Zamawiający ma na myśli pomoc w tworzeniu polityk bezpieczeństwa obowiązujących w organizacji Zamawiającego, w których Wykonawca wykorzysta szerszą niż posiada Zamawiający wiedzę na temat zapewnienia bezpieczeństwa monitorowanych systemów.

Punkt 5.3 OPZ

Czy Zamawiający może doprecyzować maksymalną ilość scenariuszy i czy zwiększanie ich powyżej minimalnych 10 będzie skutkowałem aneksowaniem istniejącej umowy?

W ramach wdrożenia usługi Zamawiający oczekuje przygotowania co najmniej 10 scenariuszy postępowania z wykrytymi incydentami. W ramach działania usługi ilość scenariuszy zależeć będzie od ilości i rodzaju wykrywanych incydentów tak, aby zapewnić sprawną klasyfikację i obsługę wykrywanych zdarzeń.

§ 2 ust. 3 Wzoru Umowy

Zamawiający w par. 2 ust. 3 wzoru Umowy zastrzega, iż można rozwiązać umowę z 3-miesięcznym okresem wypowiedzenia. Wykonawca zwraca uwagę, że z zasady umowy w zamówieniach publicznych są zawierane na czas oznaczony, a świadczenie wykonawcy winno być tożsame ze świadczeniem określonym w składanej przez niego ofercie. Wszelkie zapisy zezwalające na rozwiązanie umowy mogą spowodować, że projekt stanie się nierentowny. Czy wobec powyższego Zamawiający wykreśli powyższy zapis z treści wzoru umowy?

Zamawiający zgadza się na wykreślenie z treści Umowy zapisu § 2 ust. 3 pod warunkiem, że Wykonawca zgodzi się na rozłożenie płatności za wdrożenie usługi (składnik ceny oferty C2, ust. 4 Zapytania Ofertowego) na równe raty miesięczne płatne w całym okresie 36 miesięcy obowiązywania umowy po zakończonym okresie wdrożenia.

§ 3 ust. 11 Wzoru Umowy

Zgodnie z § 3 ust. 11 wzoru Umowy, za termin zapłaty wynagrodzenia należnego Wykonawcy uważa się dzień obciążenia rachunku Zamawiającego. Należy zwrócić uwagę, że postanowienie to w obecnym brzmieniu jest niezgodne z powszechną zasadą oraz linią orzecznictwa Sądu Najwyższego (por. uchwała SN z dn. 4 stycznia 1995 r. sygn. CZP 164/94), w myśl których za dzień spełnienia świadczenia pieniężnego w postaci bezgotówkowej uważa się dzień uznania rachunku bankowego wierzyciela (tu Wykonawcy), a nie dzień obciążenia rachunku bankowego dłużnika (tu Zamawiającego). Czy w związku z powyższym Zamawiający wyrazi zgodę na zmianę powyższego zapisu i uzna dniem zapłaty dzień uznania rachunku bankowego Wykonawcy?

Zamawiający zgadza się na zmianę zapisu §3 ust. 11 wzoru Umowy, który przyjmuje treść:
„Za termin zapłaty faktury VAT uznaje się dzień uznania rachunku bankowego Wykonawcy."

§ 4 ust. 5 Wzoru Umowy

Zamawiający w par. 4 ust. 5 wzoru Umowy wymaga zgody na potrącanie kar umownych z dowolnej należności Wykonawcy. Wykonawca zwraca uwagę, iż kary umowne winny być dochodzone po uprzednio przeprowadzonym procesie reklamacyjnym. Natomiast nieprawidłowości dotyczące płatności zawsze są regulowane fakturami korygującymi lub też notami księgowymi po rozpatrzeniu złożonej reklamacji. Czy Zamawiający wyraża zgodę na zmianę umowy poprzez dodanie zapisu o tym, że kary umowne będą naliczane po zakończeniu procedury reklamacyjnej ?

Zamawiający nie wyraża zgody na zmianę brzmienia §4 ust. 5 wzoru Umowy.

Punkt 3.5 Zapytania Ofertowego

Prosimy o potwierdzenie czy Zamawiający uzna drugi certyfikat Certified Ethical Hacking wydany przez organizację EC-Council za równoważny certyfikatowi OSCP w zakresie wymagań dotyczących osób zatrudnionych przez wykonawcę opisanych w zapytaniu ofertowym nr IT/AW/90/2023 pkt. 3.6 do SWZ ?

Zamawiający uzna drugi certyfikat CEH wydany przez EC-Council za równoważny certyfikatowi OSCP.

Punkt 5 Zapytania Ofertowego

. Wykonawca prosi o informację czy Zamawiający dopuszcza podpisanie oferty kwalfikowanym podpisem elektronicznym oraz złożenie oferty wraz z wymaganymi dokumentami poprzez platformę OpenNexus, na której zostało opublikowane postępowanie przez Zamawiającego? W wypadku zgody Czy Zamawiający dopuszcza odstąpienie od zapisu – „Poszczególne strony oferty powinny być ze sobą połączone i kolejno numerowane" ?

Zamawiający wyraża zgodę na złożenie oferty podpisanej kwalifikowanym podpisem elektronicznym osoby upoważnionej do składania oświadczeń woli w imieniu Oferenta. Jednocześnie Zamawiający dopuszcza odstąpienie od zapisu „Poszczególne strony oferty powinny być ze sobą połączone".

Wzór Umowy

. Wnosimy o dodanie w dokumencie „5. IT - UMOWA na usługi z zakresu Cybersecurity – SOC" w §6 nowego ustępu o treści:

„Administratorem danych osobowych Zamawiającego oraz jego personelu jest Wykonawca. Informacja dotycząca przetwarzania przez Wykonawcę danych osobowych stanowi Załącznik nr 6 do niniejszej Umowy. Informację Zamawiający zobowiązany jest przekazać w imieniu Wykonawcy wszystkim osobom, których dane przetwarzane będą w związku z zawarciem i wykonywaniem niniejszej umowy".

Zamawiający wyraża zgodę na dodanie w §6 Wzoru Umowy ustępu o podanej treści.

Wzór Umowy

Wnosimy o dodanie nowego Załącznika nr 6 do dokumentu „5. IT - UMOWA na usługi z zakresu Cybersecurity – SOC"

Zamawiający wyraża zgodę na dodanie do Wzoru Umowy nowego Załącznika nr 6 pod warunkiem dostarczenia jego treści Zamawiającemu i akceptacji tej treści przez Zmawiającego przed końcem postępowania.

Załącznik nr 4 do Wzoru Umowy

Wnosimy o poprawę oczywistej omyłki w Załączniku nr 4 – „Umowa o powierzeniu przetwarzania danych osobowych", tj. zmianę w §10 ust. 1 zapisu w zdaniu pierwszym oraz w zdaniu 3 z „§ 4 ust. 3" na „§ 4 ust. 4"

Zamawiający akceptuje poprawę omyłki we wskazanych miejscach Załącznika nr 4 do Wzoru Umowy.

Załącznik nr 4 do Wzoru Umowy

Wnosimy o rozszerzenie zapisów w Załączniku nr 4 – „Umowa o powierzeniu przetwarzania danych osobowych" poprzez dodanie w §10 ust. 4 zdania „Przetwarzający po zapoznaniu z przedłożonym protokołem pokontrolnym ma prawo zgłoszenia wyjaśnień lub zastrzeżeń do jego ustaleń".

Zamawiający wyraża zgodę na dodanie w §10 ust. 4 podanego zdania.

Załącznik nr 4 do Wzoru Umowy

Wnosimy o zmianę, w Załączniku nr 4 – „Umowa o powierzeniu przetwarzania danych osobowych", zapisu §11 ust. 3 w zdaniu pierwszym z „oraz posiadanych nośników elektronicznych" na „oraz na nośnikach elektronicznych".

Zamawiający wyraża zgodę na zmianę treści §11 ust. 3 Załącznika nr 4 do Wzoru Umowy.