Załącznik nr 3 do MN

Rejestr pytań i odpowiedzi

Rejestr pytań i odpowiedzi do postępowania nr **ZC/61/EITE-BB/2019**

Nr pytania	Referencja do MN	Treść Pytania	Odpowiedź EITE
1.	-	Ile urządzeń jest przewidzianych do audytowania (model. typ)?	Punkty styku z siecią Internet – łącznie 4 urządzenia (2 routery brzegowe, 2 firewalle zewnętrzne) Usługa VPN – 4 urządzenia, WAF – 3 urządzenia. Pozostałe informacje (model, typ) nie będą na obecną chwilę udostępniane (brak umowy NDA).
2.	-	Ile usług jest przewidzianych do audytowania ?	3 usługi: Punkt styku z siecią Internet, Usługa VPN, WAF.
3	-	Ile punktów styku z siecią internet Państwo posiadacie?	2
4.	Umowa główna par 9 ust. 4	Kara umowna w wysokości 100% wynagrodzenia za każde naruszenie zapisów par 12 Tajemnica przedsiębiorstwa wydaje się rażąco wysoka. Proponujemy zmniejszenie do wysokości 30% wartości wynagrodzenia	Zamawiający nie wyraża zgody na zmianę zapisów umowy.
5.	Umowa główna par 15	Prośba o zmianę zapisu z „ryzyko i tytułu własności” na zapis „ryzyko i tytuł własności”	Zamawiający nie wyraża zgody na zmianę zapisów umowy.
6.	Umowa powierzenia par 6 ust 1	Umowa powierzenia przetwarzania danych osobowych powinna przestać obowiązywać w momencie wygaśnięcia umowy głównej, nie zaś wyłącznie w razie jej rozwiązania. Umowa główna może wygasnąć w wyniku rozwiązania, ale również odstąpienia, wykonania. Z tej przyczyny	Zamawiający nie wyraża zgody na zmianę zapisów umowy.

		konieczne jest postanowienie zgodnie z którym umowa przetwarzania danych osobowych wygasa z chwilą wygaśnięcia umowy głównej bez względu czy umowa główna została rozwiązania, wykonana, czy od niej odstąpiono. Prosimy o zmianę zapisów stosownego paragrafu w Umowie powierzenia	
7.	Umowa główna par 7	Proponujemy zmianę zapisów dot. praw autorskich jak poniżej. W ramach wynagrodzenia ustalonego w Umowie na realizacje prac, Wykonawca przeniesie na Zamawiającego, bezterminowo i bez ograniczeń co do terytorium, na zasadzie wyłączności, autorskie prawa majątkowe do opinii i raportów, będących efektem Zlecenia prac (utworów) na wszelkich polach eksploatacji w rozumieniu przepisów o prawie autorskim i prawach pokrewnych. Jednocześnie przeniesienie na Zamawiającego autorskich praw majątkowych do opinii i raportów, będących przedmiotem Zlecenia, o których mowa powyżej, nie będzie skutkowało przeniesieniem na Zamawiającego praw własności intelektualnej lub innych praw majątkowych do narzędzi, systemów, metodyk, metodologii, koncepcji, wzorców, programów komputerowych oraz know-how (Wiedza Wykonawcy) użytych przez Wykonawcę. Przeniesienie praw autorskich nie będzie ograniczała Wykonawcy w żaden sposób w używaniu Wiedzy Wykonawcy w jego działalności, w tym na rzecz innych podmiotów, jak również tworzenia na ich podstawie materiałów podobnych do rezultatów prac dostarczonych Zamawiającemu w ramach wykonania Zamówienia. Chcielibyśmy uniknąć sytuacji przeniesienia praw autorskich na metodyki, know-how itp. które to uniemożliwiałoby nam w przyszłości wykonywanie podobnych projektów.	Zamawiający nie wyraża zgody na zmianę zapisów umowy.
8.	Materiały negocjacyjne Załącznik nr 1 pkt 1 Punkt styku z siecią Internet	Jakie urządzenia (np. routery CISCO) będą wchodzić w zakres testów punkcie nr. 1. Punkty styku z siecią Internet ?	Na obecnym etapie postepowania Zamawiający nie ujawnia informacji tego typu informacji (brak umowy NDA).

9.	Materiały negocjacyjne Załącznik nr 1 pkt 2 Dostęp do infrastruktury za pośrednictwem VPN	Jakie oprogramowania/urządzenia (np. Cisco VPN, Palo Alto VPN, WireGuard, IPSec, OpenVPN, Algo, etc.) będą wchodzić w zakres testów w punkcie nr. 2. Dostęp do infrastruktury za pośrednictwem VPN (Virtual Private Network) ?	Na obecnym etapie postepowania Zamawiający nie ujawnia informacji tego typu informacji (brak umowy NDA).
10.	Materiały negocjacyjne Załącznik nr 1 pkt 3 Web Application Firewall	Jakie urządzenia/oprogramowanie (np. Imperva WAF, F5, etc.) będzie wchodzić w zakres testów w punkcie nr. 3 Web Application Firewall (WAF)?	Na obecnym etapie postepowania Zamawiający nie ujawnia informacji tego typu informacji (brak umowy NDA).
11.	Materiały negocjacyjne Załącznik nr 1 pkt II	Czy testy White-box będą dotyczyć tylko urządzeń z punktów 1-3: • Z punktu nr 1. Punkty styku z siecią Internet - 4 urządzenia (2 routery brzegowe, 2 firewalle zewnętrzne). • Z punktu nr 2 Dostęp do infrastruktury za pośrednictwem VPN - 4 urządzenia VPN. • Z punktu nr 3. Web Application Firewall - 3 urządzenia WAF. Jeżeli testy White-box będą dotyczyć także innych urządzeń to prośba o podanie ich ilości i typów M	Tak, testy dotyczą tylko wskazanych obszarów.
12.	Materiały negocjacyjne Załącznik nr 1 pkt I	Czy testy Black-box będą dotyczyć tylko 20 adresów IP ,w obrębie których będą występować wszystkie urządzenia z punktów 1-3: • Z punktu nr 1. Punkty styku z siecią Internet - 4 urządzenia (2 routery brzegowe, 2 firewalle zewnętrzne). • Z punktu nr 2 Dostęp do infrastruktury za pośrednictwem VPN - 4 urządzenia VPN. Z punktu nr 3. Web Application Firewall - 3 urządzenia WAF.	Tak.
13.	-	Czy zamawiający dopuszcza przeprowadzenie testów penetracyjnych z pominięciem fazy BLACKBOX - takie testy wydłużą czas realizacji takiego zlecenia, a w świetle obecnej praktyki odchodzi się od testów jakim poddawana jest infrastruktura codziennie :) z uwagi na jej udostepnienie po stronie internetu	Nie.

14.	IV pkt 3	Zamawiający wymaga, aby dostarczony produkt spełniał (obowiązujące na dzień odbioru) przepisy dotyczące ochrony danych osobowych. Prosimy o doprecyzowanie oczekiwania	Chodzi o zgodność z powszechnie obowiązującym Rozporządzeniem w sprawie ochrony danych osobowych.
15.	Miejsce realizacji	Czy prace mogą być realizowane w sposób zdalny ? W dokumencie jest zdanie "Prace związane z wykonywaniem przedmiotu zamówienia będą odbywać się w miejscu wskazanym przez Zamawiającego, na terenie podmiotów wchodzących w skład Grupy ENERGA."	Zamawiający dopuszcza zdalną realizację testów blackbox. Pozostałe testy należy wykonać w lokalizacji Zamawiającego.
16.	Załącznik nr 1 do materiałów negocjacyjnych pkt. 1. - metodyki	Prosimy o doprecyzowanie oczekiwań Zamawiającego w zakresie metodyk, którymi posiłkować się ma Wykonawca w trakcie realizacji zadań objętych zapytaniem Czy Zamawiający oczekuję, iż Wykonawca wykorzysta wszystkie poniższe metodyki: • Open Source Security Testing Methodology Manual (Herzog, 2006) • Information Systems Security Assessment Framework (OISSG, 2006) • Penetration Testing Execution Stanard (PTES, 2015) • OWASP TOP 10 methodology (OWASP, 2017) • NIST SP 800-115 standard (NIST, 2008). • Payment Card Industry Data Security Standard (PCI DSS)	Zamawiający wskazując metodyki oczekuje takiego ich doboru, zgodnie z najlepszymi praktykami i doświadczeniem Wykonawcy aby przedstawiony końcowy raport testów był odpowiadający stanowi faktycznemu.
17.	Załącznik nr 1 do materiałów negocjacyjnych pkt. 2.	Jakie inne metodyki Zmawiający ma jeszcze na myśli a o których wspomina :" Powyższa lista nie wyczerpuje zakresu oczekiwanych metodologii. Wykonawca może zaproponować metodologię testów pod założonym warunkiem oparcia o powszechnie obowiązujące normy i standardy prowadzenia testów bezpieczeństwa."	Zamawiający założył, że Wykonawca, dysponując doświadczeniem z wcześniejszych prac może używać innych uznanych metodyk, nie wskazanych na liście. Decyzja o ich użyciu została pozostawiona Wykonawcy.
18.	Załącznik nr 1 do materiałów negocjacyjnych pkt. 1.	Czy Zamawiający ma odnieść się w trakcie testu oraz raporcie bezpośrednio do każdej z metodyk czy może się nimi jedynie posiłkować?	Zamawiający zakłada, że Wykonawca dokona wyboru najlepszej w jego ocenie metodyki, która najbardziej precyzyjnie bada dany obszar. Zamawiający nie wymaga stosowania wszystkich metodyk jednocześnie. Tak, można się wyłącznie posiłkować innymi metodykami w trakcie testu i w raporcie.
19.	Załącznik nr 1 do materiałów negocjacyjnych pkt. 1,2	Dodatkowo należy mieć na względzie część z wspomnianych "metodyk" będzie pokrywać cześć może nie mieć zastosowania do przedmiotu zapytania.	Tak, Wykonawca może sam zaproponować metodykę, która według jego wiedzy jest najlepszą do osiągnięcia zamierzonego celu.

		Czy Wykonawca może sam zaproponować metodyki, które wykorzysta z trakcie testu?	
20.	Załącznik nr 1 do materiałów negocjacyjnych pkt. 2.	"w ramach pracy Wykonawca opracuje wnioski audytowe oraz rekomendacje dalszych działań i koniecznych zmian odnoszących się do zidentyfikowanych niezgodności mogących doprowadzić do skutecznego przeprowadzenia cyberataku na infrastrukturę Zamawiającego uwzględniając zapewnienie zgodności działania poddanych audytowi zasobów z wymaganiami normy ISO 27001. Wnioski te będą stanowiły część końcowego raportu z audytu" O ile wiemy ISO/IEC 27001 nie narzuca wymogów dotyczących samych testów. Nie można wystawić po testach certyfikatu/ zgodność, że testy były wykonane w duchu z ISO. Najważniejsze jest aby: • testy były wykonywane regularnie - np. uwzględnione w cyklu życia oprogramowania • wyciągać wnioski z testów tzn. łatać znalezione podatności • dokumentować testy, retesty - tak żeby pochwalić się podczas certyfikacji • zapisać w nadrzędnych politykach konieczność wykonywania regularnych testów bezpieczeństwa Proponujemy by Zamawiający doprecyzował oczekiwanie.	Zamawiający nie oczekuje certyfikatu zgodności testów z normą ISO 27001. Zamawiający oczekuje, że wymogi tej normy będą uwzględnione podczas realizacji testów, a potencjalne wykryte niezgodności względem tej normy zostaną przedstawione w raporcie.
21.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.1	Jakie adresy IP zewnętrzne posiada klient?	IP v4. Pozostałe informacje, ujawniające elementy infrastruktury Zamawiającego nie będą na tym etapie ujawnione (brak umowy NDA).
22.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.1	Czy klient posiada łącza o zmiennych adresach IP zewnętrznych? Np. urządzenia korzystające z Internetu mobilnego/Neostrada?"	Nie.
23.	Załącznik nr 1 do materiałów negocjacyjnych Zakres	Czy w sieci klienta znajdują się jakieś systemy zabezpieczenia przykład IPS/IDS? Jeżeli tak to jakie?"	Informacje, ujawniające elementy infrastruktury Zamawiającego nie będą na tym etapie ujawnione (brak umowy NDA).

	techniczny testów penetracyjnych pkt.1		
24.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.1	Czy w sieci klienta znajdują się adresy IP, które powinny zostać wykluczone z testów? Jeżeli tak to jakie?	Tak, w sieci Zamawiającego znajdują się adresy IP, które powinny zostać wykluczone. Informacje, ujawniające elementy infrastruktury Zamawiającego nie będą na tym etapie ujawnione (brak umowy NDA).
25.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.1	Ile poglądowo klient posiada zewnętrznych adresów IP?	Do testów wskazane zostanie 20 publicznych adresów IP. Pozostałe informacje, ujawniające elementy infrastruktury Zamawiającego nie będą na tym etapie ujawnione (brak umowy NDA).
26.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.2	Prosimy o precyzyjne wskazanie liczby urządzeń objętych niniejszym zadaniem oraz ich rodzaj.	Punkty styku z siecią Internet – łącznie 4 urządzenia (2 routery brzegowe, 2 firewalle zewnętrzne) Usługa VPN – 4 urządzenia, WAF – 3 urządzenia. Pozostałe informacje (model, typ) nie będą na obecną chwilę udostępniane (brak umowy NDA).
27.	Załącznik nr 1 do materiałów negocjacyjnych Zakres techniczny testów penetracyjnych pkt.3	Web Application Firewall (WAF) Prosimy o precyzyjne wskazanie liczby urządzeń objętych niniejszym zadaniem.	WAF – 3 urządzenia.
28.	Zakres techniczny testów penetracyjnych	Czy Wykonawca będzie miał możliwość również ewentualnego, samodzielnego dostępu do urządzeń objętych audytem?	Dostęp do urządzeń będzie odbywać się wyłącznie pod bezpośrednim nadzorem Zamawiającego.

29.	Zakres techniczny testów penetracyjnych	Czy będzie mógł manualnie potwierdzić wyniki analizy/ Czy będzie mógł wykorzystać narzędzia takie jak nessus?	Zamawiający nie narzuca ograniczeń w zakresie używanych narzędzi. Cześć pytania dotycząca manualnego potwierdzenia wyników analizy nie jest dla Zamawiającego zrozumiała.
30.	-	Prosimy o informację czy wycena testów powinna zostać podzielona dla poszczególnych zadań tzn. osobno black - box, osobno white – box.	Zamawiający oczekuje wyceny całości prac.
	Załącznik nr 1	" [PŁATNOŚĆ]: II ETAPY: I. Po przeprowadzeniu testów, dostarczeniu raportu zaakceptowanego przez Zamawiającego oraz protokołu odbioru – 60% wynagrodzenia, II. Po przeprowadzeniu retestów dostarczenia raportu zaakceptowanego przez Zamawiającego oraz protokołu odbioru – 40% wynagrodzenia." Zgłaszamy się z wnioskiem o zmianę warunków płatności. Proponujemy rozliczenie proporcjonalnie do realizacji prac.	Zmawiający nie wyraża zgody na zmianę warunków płatności.
31.	Załącznik Nr 1	Czy Zmawiający uzna za wystarczające przekazanie informacji nt. członków zespołu tj. certyfikaty, lata doświadczenia, rodzaj kompetencji i doświadczenia. Bez konieczności podawania projektów w których uczestniczył dany członek zespołu.	Zamawiający oczekuje informacji zgodnie z przekazanym dokumentem RFI.
32.	Załącznik Nr 1	Zgłaszamy się z prośbą o usunięcie wymogu przekazania imienia i nazwiska oraz numeru telefonu osoby po stronie Zamawiającego (dla którego realizowany był projekt)	Zamawiający oczekuje informacji zgodnie z przekazanym dokumentem RFI.
33.	Załącznik Nr 1	Czy Zamawiający dopuszcza negocjację zapisów umowy w kolejnych etapach. Wzór umowy nie ma wszak wszystkich wartości jak np. terminy odbioru.	Zamawiający nie dopuszcza negocjowania treści umowy w kolejnych etapach.
34.	Załącznik Nr 1	Czy Wykonawca może wraz z ofertą przekazać propozycję zmian / uzupełnień zapisów?	Zamawiający nie dopuszcza zmian w umowie.
35.	IV pkt 3	Zamawiający wymaga, aby dostarczony produkt spełniał (obowiązujące na dzień odbioru) przepisy dotyczące ochrony danych osobowych. Prosimy o doprecyzowanie oczekiwania	Chodzi o zgodność z powszechnie obowiązującym Rozporządzeniem w sprawie ochrony danych osobowych.
36.	Par. 4 ust. 3 wzoru Umowy	Wykonawca dokona prezentacji wykonanych prac dla wskazanych przez Zamawiającego organów spółek z Grupy ENERGA – proszę o wyjaśnienie szczegółów realizacji lub o usunięcie zapisu.	Wykonawca dokona prezentacji raportu, wraz z jego omówieniem dla wybranych przez Zamawiającego organów spółek z Grupy Energa.
37.	Par. 9 ust. 2 wzoru Umowy	Proszę o zmianę sformułowania „opóźnienie” na „zwłokę”.	Zamawiający nie wyraża zgody na zmianę zapisów umowy.

38.	Par. 9 ust. 4 wzoru Umowy	Proszę o obniżenie wysokości kary umownej do 20% wynagrodzenia. Kara w wysokości 100% wynagrodzenia za każdy przypadek naruszenia zasad poufności jest rażąco niewspółmierna.	Zamawiający nie wyraża zgody na zmianę zapisów umowy.
39.	Par. 9 ust. 6 wzoru Umowy	Proszę o ustanowienie limitu odpowiedzialności Wykonawcy z tytułu niewykonania lub nienależytego wykonania. Umowy na poziomie 20% wartości wynagrodzenia.	Zamawiający nie wyraża zgody na zmianę zapisów umowy.