Rejestr pytań i odpowiedzi do postępowania nr ZC/62/EITE-BI/2019

Nr pytania	Referencja do MN	Treść Pytania	Odpowiedź EITE
1.	ZC/62/EITE-BI/2019	Na Państwa stronie internetowej „https://bip.energa.pl/przetargi-zamowienia-i-ogloszenia/455665/zc-62-eite-bi-2019-postepowanie-niepubliczne-monitorowanie-zagrozen” dostępne są dwa pliki do pobrania, których treść jest ta sama. Czy dysponują Państwo dodatkowym szczegółowym opisem przedmiotu zamówienia (OPZ) w celu doprecyzowania zakresu przedmiotu?	Zamawiający wyjaśnia, że na stronie internetowej bip.energa.pl zamieszczone zostały dwa pliki do pobrania, o różnej treści, przy czym plik o nazwie” ZC_62_EITE-BI_2019 - Materiały Negocjacyjne_Monitorowanie zagrożeń jest dokumentem zawierającym wszelkie informacje niezbędne do przystąpienia do udziału w postępowaniu, natomiast plik o nazwie: „ZC_62_EITE-BI_2019 – Załączniki nr 2 – 4 do MN_wersja do edycji, zawiera załączniki do wypełnienia przez Wykonawców i został załączony w celu ułatwienia złożenia oferty. Opis przedmiotu zamówienia znajduje się w Załączniku nr 1 do Materiałów Negocjacyjnych.
2.	Monitorowania zagrożeń dotyczących „constituency” (wskazana adresacja publiczna IP wraz z routingiem BGP, wskazane domeny pocztowe i strony WWW) Grupy Energa	Prosimy o szczegółowe wyjaśnienie, o jakie zagrożenia pyta Zamawiający w niniejszym punkcie.	Wszelkie podszycia, przekierowania ruchu oraz ataki DDOS.
3.		Czy zagrożenia te mają być monitorowane za pomocą dedykowanych rozwiązań instalowanych przez Oferenta po stronie infrastruktury Zamawiającego, czy monitorowanie ma odbywać się po stronie informacji dostępnych u Operatora telekomunikacyjnego w zakresie routingu z adresacją Zamawiającego?	Zamawiający wyjaśnia, że nie wymaga monitorowana zagrożeń za pomocą dedykowanych rozwiązań instalowanych przez Wykonawcę po stronie infrastruktury Zamawiającego. W zakresie drugiej części pytania Zamawiający wyjaśnia, że chodzi o kompleksowy monitoring routingu BGP naszych sieci (np. w celu wykrywania nieautoryzowanego przekierowania ruchu przez podmioty obce)
4.		Prosimy o wskazanie domen pocztowych i stron WWW Grupy Energa, których ma dotyczyć monitoring, o który pyta Zamawiający.	Ilości adresów IP: około 750 Ilość domen pocztowych: około 20 Ilość stron www: około 125.

5.	Monitorowanie sieci Internet pod kątem ofert sprzedaży i zakupu danych, należących do Grupy Energa, których zawartość może świadczyć o nieuprawnionym wejściu w ich posiadanie	Prosimy o wskazanie założeń co do monitorowania sieci Internet, których w ofertach oczekuje Zamawiający.	Oferowanie lub udostępnianie danych Grupy Energa, które nie zostały podane do wiadomości publicznej.
6.		W jakim trybie Zamawiający będzie rozliczał tę usługę, czy będzie to opłata miesięczna za analizę danych w sieci internet, czy będzie to opłata za dostarczoną informację zarejestrowaną i dostarczoną do Zamawiającego przez zespół Oferenta?	Zamawiający wyjaśnia, że będzie rozliczał tę usługę w ramach opłaty miesięcznej.
7.	Monitorowanie i obsługiwanie incydentów zgłaszanych wzajemnie przez obie Strony	Czy Zamawiający posiada infrastrukturę klasy SIEM do monitorowania i obsługi incydentów?	Pytanie nie związane z przedmiotem zamówienia.
8.		Czy zakresem tego monitorowania jest infrastruktura IT czy OT, czy obydwa zakresy ?	Obydwa zakresy
9.		Czy Zamawiający może udostępnić Oferentom zakres infrastruktury, ilość danych w GB, ilość zdarzeń na sekundę (EPS), która ma zostać objęta procesem monitorowania incydentów lub która jest po stronie Zamawiającego objęta procesem monitorowania incydentów? Chodzi o tak zwane Źródła systemu klasy SIEM.	Zamawiający nie udostępnia takich danych.
10		Czy Zamawiający może wskazać Oferentom zakres scenariuszy bezpieczeństwa, które obecnie funkcjonują w procesie monitorowania incydentów bezpieczeństwa w infrastrukturze Zamawiającego lub scenariuszy bezpieczeństwa, które oczekuje Zamawiający od Oferentów?	Zamawiający nie udostępnia takich danych.
11		Czy Zamawiający może wskazać oczekiwany od Oferentów model świadczenia usługi monitorowania incydentów (zakup infrastruktury od Oferenta (IaaS) / zakup infrastruktury i oprogramowania przez Oferenta (SaaS) / model usługowy (MSSP))?	Model usługowy.
12		Czy Zamawiający preferuje producenta oprogramowania systemu klasy SIEM po stronie Oferenta (dostarczenie lub model usługowy) ?	Pytanie nie związane z przedmiotem zamówienia.

13		Jeżeli Zamawiający posiada wdrożony i funkcjonujący system klasy SIEM, to prosimy o wskazanie jego architektury z uwzględnieniem całej infrastruktury podłączonej do niego w celu monitorowania incydentów.	Pytanie nie związane z przedmiotem zamówienia.
14		Czy Zamawiający zakłada proces monitorowania po stronie swojej i Oferenta z uwzględnieniem zespołu operacyjnego (np. Security Operations System) ? Jeżeli tak, to prosimy o wskazanie, gdzie dany zespół będzie świadczył usługi operacyjne? Czy po stronie Zamawiającego czy po stronie Oferenta ? Czy po każdej ze stron?	Nie
15		Czy Zamawiający zakłada proces monitorowania po swojej stronie i Oferenta z uwzględnieniem tylko i wyłącznie Operatorów (jedynie notyfikacje) czy też Analityków (analiza w oparciu o dane z systemów Zamawiającego), czy również udział ekspertów bezpieczeństwa?	Zapytanie dotyczy zewnętrznego monitoringu bezpieczeństwa.
16		Jakich kompetencji wymaga Zamawiający od Oferenta w celu świadczenia usługi?	Kompetencje niezbędne do realizacji zadań będących przedmiotem zamówienia na poziomie eksperckim.
17		Czy możemy prosić o założenia lub kompletny proces zakładany przez Zamawiającego w procesie monitorowaniu incydentów?	Zamawiający nie udostępnia takich danych
18		W jakim modelu Zamawiający zakłada świadczenie usługi? 24/7/365? Prosimy o wskazanie.	Monitoring automatyczny: 24/7/365 Dostępność ekspertów: 8/5 (godziny robocze)
19		Jakiego systemu biletowania/obsługi incydentów używa Zamawiający?	Pytanie nie związane z przedmiotem zamówienia.
20		W przypadku funkcjonowania systemu SIEM po stronie Zamawiającego i konieczności uruchomienia procesu monitorowania infrastruktury Zamawiającego po stronie Oferenta czy Zamawiający dopuszcza integracje tych systemów?	Przedmiot niniejszego zamówienia nie dotyczy wewnętrznych systemów Zamawiającego.
21	Wsparcie przy analizie złośliwego oprogramowania i podejrzanych e-maili (m.in. wektory ataku,	Jakiego wsparcia i w jakim modelu oczekuje Zamawiający od Oferenta?	- Analiza charakteru podejrzanej wiadomości, - Analiza zagrożeń zawartych w wiadomości (np. rodzaj zagrożenia w przesłanych załącznikach, analiza zagrożeń dotycząca linków zawartych w email),

	związane z tym zagrożenia) oraz dostarczanie stosownych wskaźników IoC będących wynikiem tychże analiz		-skala potencjalnego ataku (np. czy jest to fragment od dłuższego czasu obserwowanej kampanii), - Analiza wektorów ataku (adresy IP, nazwy domen DNS, adresy pocztowe) Czas reakcji - nie dłużej niż 4 godziny.
22		W jaki sposób Zamawiający dostarczać będzie złośliwe oprogramowanie do Oferenta w celu jego analizy?	Przesłanie drogą mailową na wskazany adres przez Dostawcę (potencjalny malware zabezpieczony hasłem).
23		Prosimy o wskazanie przykładowego IoC oraz e-maila przez Zamawiającego.	Zamawiający nie widzi konieczności udostępniania takich danych na tym etapie procesu zakupowego.
24		W jakim modelu czasowym Zamawiający oczekuje świadczenia usługi?	Zgodnie z odpowiedzią na zapytanie nr 21 powyżej.
25	Informowanie o wykrytych podatnościach w oprogramowaniu, systemach IT i sprzęcie OT oraz dostarczanie propozycji ich mitygacji	Czy Zamawiający dysponuje specjalistyczną infrastrukturą dla systemów IT/OT dedykowaną do wykrywania podatności, czy oczekuje dostarczenia tej infrastruktury od Oferenta? Jeżeli dostarczenia, to prosimy o informacje jaki model rozliczenia i świadczenia usług jest preferowany / oczekiwany od Zamawiającego.	Zamawiający nie oczekuje dostarczenia takiej infrastruktury przez Wykonawcę.
26		Jakie są założenia Zamawiającego do monitorowania podatności w systemach IT / OT?	Zostanie dostarczona lista na poziomie producentów: systemów IT i sprzętu OT.
27		Czego dokładnie oczekuje Zamawiający od Oferenta pod pojęciem „dostarczanie propozycji ich mitygacji”? Prosimy o przykłady do identyfikowanych przez Zamawiającego zagrożeń.	Np. propozycja rozwiązania obejściowego do czasu przygotowania poprawek przez producenta.
28	Konsultacje w zakresie wsparcia merytorycznego przez pracowników Dostawcy	Prosimy o wskazanie merytorycznego zakresu oczekiwanego wsparcia. Czy wsparcie ma być dostarczone w usłudze Oferta dla pracowników Zamawiającego?	Zakres: bezpieczeństwo sieci, systemów operacyjnych i oprogramowania. Wsparcie ma być dostarczone w usłudze - w ilości średnio 5 godzin m-ce, w trybie 8/5.
29		Prosimy o wskazanie ilości pracowników Zamawiającego oraz ich miejsca świadczenia pracy na terenie Kraju lub Świata	Zamawiający nie widzi konieczności udostępniania takich danych na tym etapie procesu zakupowego.

30		Czy oczekiwane usługi mają być realizowane w trybie zdalnym? e-learningowym? telefonicznym, czy mają być przeprowadzane szkolenia? Jeżeli szkolenia, to prosimy o wytyczne co do założeń Zamawiającego gdzie i w jakiej ilości mają być przeprowadzane, czego dotyczyć i jak często.	Konsultacje w trybie zdalnym; nie chodzi o szkolenia, a raczej doradztwo.
31	Blokowanie, usuwanie i minimalizacja skutków ataków na infrastrukturę teleinformatyczną Grupy Energa	Prosimy o wskazanie modelu świadczenia usług.	Model usługowy.
32		Czy Zamawiający posiada infrastrukturę do blokowania, usuwania i minimalizowania skutków ataków na infrastrukturę teleinformatyczną Grupy Energa? Jeżeli tak, to prosimy o wyszczególnienie.	Pytanie nie związane z przedmiotem zamówienia.
33		Prosimy o założenia Zamawiającego co do modelu świadczenia usług, model wdrożenia, model usługowy ?	Zgodnie z odpowiedzią na zapytanie nr 31 powyżej.
34		Prosimy o przedstawienie architektury infrastruktury teleinformatycznej Grupy Energa za zaznaczonymi punktami styku z sieciami wewnętrznymi (IT/OT) oraz punktami styków z sieciami zewnętrznymi w tym z siecią internet.	Pytanie nie związane z przedmiotem zamówienia.
35	Natychmiastowe informowanie przez Dostawcę o IP urządzeń Grupy Energa zarażonych złośliwym oprogramowaniem	Czy Zamawiający posiada dedykowane rozwiązania anty wirusowe lub anty malware'owe ? Jeżeli tak, to jakie ?	Pytanie nie związane z przedmiotem zamówienia.
36		Czy Zamawiający oczekuje dostarczenia dedykowanej infrastruktury do sieci IT/OT, czy realizowania usługi w formie usługowej ?	Zamawiający nie oczekuje dostarczenia dedykowanej infrastruktury do sieci IT/OT. Realizacja zamówienia w formie usługowej.
37	Monitorowanie pojawiania się i natychmiastowe informowanie o podatnościach 0-day i wszelkiego rodzaju błędów mogących dotyczyć oprogramowania, mikrokodu i sprzętu	Czy Zamawiający posiada dedykowane rozwiązania typu sandbox, analizatory kodów źródłowych, skanery podatności ? Jeżeli tak, to jakie ?	Pytanie nie związane z przedmiotem zamówienia.
38		Czy Zamawiający oczekuje dostarczenia dedykowanej infrastruktury do monitorowania sieci IT/OT, czy realizowania usługi w formie usługowej ?	Zamawiający nie oczekuje dostarczenia dedykowanej infrastruktury do monitorowania sieci IT/OT. Realizacja zamówienia w formie usługowej.

39	wykorzystywanego w Grupie Energa	Prosimy o wskazanie języków programowania oprogramowania w grupie Energa	Pytanie nie związane z przedmiotem zamówienia.
40		Co oznacza mikrokod?	Firmware. Oprogramowanie działające poniżej jądra systemu operacyjnego.
41		Prosimy o przedstawienie listy sprzętu, którego ma dotyczyć usługa monitorowania	Lista taka zostanie dostarczona na etapie uzgadniania warunków umowy (po podpisaniu stosownych umów NDA).
42		Prosimy o doprecyzowanie, jakie błędy ma na myśli Zamawiający pisząc, że mogą dotyczyć oprogramowania, mikrokodu i sprzętu wykorzystywanego w Grupie Energa.	Wszelkie błędy oprogramowania, systemów operacyjnych i firmware dotyczących listy producentów, która zostanie przekazana na późniejszym etapie.
43	Pkt IV.1b	Jakie wymagania stawia wykonawca zespołowi, który będzie realizował usługę? Czy jest wymagane doświadczenie pracy w Security Operations Center lub posiadanie certyfikatów?	Zgodnie z odpowiedzią na zapytanie nr 16 powyżej.
44	Pkt IV.1b	Czy usługa ma być realizowana przez pracowników zatrudnionych przez Wykonawcę? Czy mogą to być pracownicy kontraktowi (B2B)?	Nie wymagamy zatrudnia ekspertów w formie umowy o pracę.
45	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 1-9	W jakim trybie ma być świadczona usługa? 8h/5 dni roboczych? 24h/dobę/365 dni w roku?	Zgodnie z odpowiedzią na zapytanie nr 18 powyżej.
46	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 1-9	Jakie jest wymagane SLA dla obsługi zgłaszanych przez Zamawiającego incydentów?	Zgodnie z odpowiedzią na zapytanie nr 21 powyżej.
47	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 1	Jakie źródła ma obejmować usługa monitoringu zagrożeń? Czy mowa tutaj o ogólnodostępnych zasobach internetowych, czy obejmuje również tzw. Deepweb/darkweb? Ile jest stron WWW, domen pocztowych i jakie klasy adresowe domeny publicznej mają być objęte monitorowaniem?	Monitoring ma również obejmować Deepweb/darkweb; Ilość podana w pkt 4.

48	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 2	Jaki zakres danych ma podlegać monitorowaniu? Czy chodzi o konkretny rodzaj (osobowe, finansowe, logowania, systemów informatycznych)?	Zgodnie z odpowiedzią na zapytanie nr 5 powyżej.
49	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 3	Czy Zamawiający zakłada różne kategorie incydentów w zależności od wpływu na organizację? Jakie będą kryteria wpływające na klasyfikację incydentu?	Zamawiający nie rozważa klasyfikacji.
50	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 3	Kto zajmuje się priorytetyzacją zgłoszeń? Czy jest to pracownik odpowiedzialny za bezpieczeństwo po stronie Zamawiającego?	Pracownik Bezpieczeństwa Zamawiającego w ewentualnej konsultacji z Dostawcą.
51	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 3	W jaki sposób Wykonawca ma zgłaszać incydenty Zamawiającemu? Czy oznacza to, że w ramach usługi ma również uwzględnić integrację systemów obsługi incydentów?	Zgłaszanie incydentów będzie odbywać się poprzez przesłanie drogą email na adres cert@energa.pl.
52	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 4-5	W jakiej formie Zamawiający chciałby otrzymywać informacje o znalezionych zagrożeniach, wskaźnikach IoC, wykrytych podatnościach, itd.? W jakich formatach mają być przekazywane? Czy będą importowane do systemów Zamawiającego? Jeśli tak, to do jakich?	Przesłanie drogą email na adres cert@energa.pl. Preferowany format CVS.
53	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 5	Bazując na doświadczeniu Zamawiającego, jak szacowana jest średnia ilość incydentów do obsługi w ciągu miesiąca? Ile z tych incydentów mogłyby mieć odpowiednio wysoki status (high, critical)?	Szacowana średnia ilość incydentów wynosi kilka w miesiącu.
54	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 5	Czy Zamawiający posiada własne systemy bezpieczeństwa, które mają zostać podłączone do systemów Wykonawcy? Jakiego rodzaju są to systemy? Ile ich jest i z ilu lokalizacji będą wysyłane informacje do systemów Wykonawcy? Czy wykrywanie podatności ma się opierać na skanowaniu automatycznym? Jeśli tak, to czy odpowiednie oprogramowanie i licencje ma być dostarczone przez Wykonawcę? Jaka jest liczba koniecznych do przeskanowanych adresów IP?	Zamawiający nie będzie podłączał własnych systemów bezpieczeństwa, do systemów Wykonawcy. Liczba adresów IP została podana w pkt 4 powyżej.

55	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 6	Jakiego rodzaju wsparcie merytoryczne jest wymagane przez Zamawiającego? Jakie obszary i zakresy ma obejmować (prawne, organizacja zespołów bezpieczeństwa, audytowe, eksperckie techniczne, eksperckie prawne, eksperckie w zakresie konkretnych systemów, typów rozwiązań technicznych)?	Wsparcie eksperckie techniczne i w zakresie konkretnych systemów, urządzeń i oprogramowania.
56	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 7	Czy blokowanie, usuwanie i minimalizacja skutków ataku ma być realizowana osobiście w lokalizacjach Zamawiającego? Jeśli tak to w ilu i w jakich miejscowościach? Jakie jest wymagane SLA i zakres oczekiwanego wsparcia?	Usługa ta nie będzie realizowana osobiście w lokalizacjach Zamawiającego. Czas reakcji - nie dłużej niż 4 godziny w trybie 8/5. Zakres: wsparcie w przeciwdziałaniu skutkom ataku oraz rekomendacje dotyczące działań prewencyjnych (w formie pisemnej)- przesłane drogą email na adres cert@energa.pl.
57	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 7	Czy Zamawiający zakłada, że w ramach postępowania zostaną dostarczone urządzenia, systemy, licencje, niezbędne do realizacji usługi? Jeśli to, to z jakimi systemami ma się integrować?	Nie.
58	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 8-9	Co oznacza kilkukrotnie pojawiające się sformułowanie „natychmiastowe” w powyższym zapytaniu?	Natychmiast po wykryciu.
59	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 8-9	Na jakiej zasadzie ma być realizowane zadanie (w oparciu o monitorowanie wodopojów, pasywne skanowanie transmisji, monitorowanie deepnetu/darknetu, itp.)?	W oparciu o dostępne zewnętrzne źródła.
60	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 9	Jaka jest liczba obiektów, których miałoby dotyczyć monitorowanie? Czy Zamawiający ma precyzyjnie zinwentaryzowane zasoby i czy jest w stanie przedstawić typy i rodzaje sprzętu, oprogramowanie i wersje?	Zamawiający, po zawarciu umowy, dostarczy listę na poziomie producentów: systemów IT i sprzętu OT. Szacujemy około 60 różnych producentów i sumaryczne 100 różnych produktów i rozwiązań.

61	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 10	W jakiej formie (osobistej, mailowej) jest przekazywany raport i komu? Specjalistom od cyberbezpieczeństwa, administratorom systemów? Osobom decyzyjnym?	Na skrzynkę cert@energa.pl. Dla ekspertów od cyberbezpieczeństwa.
62	Załącznik nr 1 do MN – Opis przedmiotu zamówienia, pkt 1. tiret 10	Jak duży zakres szczegółowości ma przedstawiać raport? Czy jest przewidziany zatwierdzony wzór raportu? Jakie są wymagane elementy, które musi zawierać?	Lista usług, statystyka przesyłanych zgłoszeń z podziałem na kategorie: zapytania i zgłoszenia od Zamawiającego, zdarzenia dotyczące zasobów Zamawiającego (wraz z skróconą analizą rozgłoszeń prefiksów sieci Zamawiającego w BGP), Informacje o zagrożeniach z podziałem na kategorie.
63	Załącznik Nr 1	W jaki sposób Zamawiający rozumie „blokowanie, usuwanie i minimalizacja skutków ataków na infrastrukturę teleinformatyczną Grupy Energa” jeśli Dostawca ni będzie miał dostępu do systemów bezpieczeństwa Zamawiającego.	Na podstawie informacji, które są możliwe do uzyskania ze źródeł zewnętrznych.