Rozdział I. Przedmiot Zamówienia

1.1. Część nr 1 zamówienia - przedmiotem zamówienia jest świadczenie przez Wykonawcę usługi polegającej na opracowaniu scenariuszy cyberzagrożeń, planów działania i procedur obsługi zdarzeń
w Organizacji, w wyniku której Wykonawca opracuje Raport końcowy.

W ramach usługi Wykonawca Opracuje:

1.1.1. Następujące scenariusze:

1) Scenariusz ataku typu Ransomware;

2) Scenariusz ataku typu DDoS/długotrwały atak;

3) Scenariusz ataku na aplikacje webowe ARiMR dostępne z poziomu Internetu;

4) Scenariusz ataku Phishingowego;

5) Scenariusz odnośnie podejrzanej aktywności sieciowej.

Dla każdego z opisanych scenariuszy, z uwzględnieniem wektora ataku, należy przygotować przystępną graficzną reprezentację kolejnych etapów ataku oraz odpowiadających im technik i taktyk obronnych. Dokumenty powinny uwzględniać zastosowanie frameworku Kill Chain, matrycy Mitre ATT&CK oraz Model Diamentowy.

1.1.2. Procedury i plany działań muszą być uniwersalne (dopuszczalne jest wpisanie narzędzi, które już posiada Organizacja), umożliwiające realizację na różnych systemach (procedury nie mogą być vendor-lock). Każda z procedur powinna zawierać maksymalnie trzy scenariusze ataku.

1.1.3. Każdy ze scenariuszy powinien zawierać zakres detekcji i odpowiedzi na sytuacje ze scenariuszy:

Zakres detekcji:

1) Opis technik oraz taktyk wskazanych w matrycy MITRE ATT&CK, które powinny zostać uwzględnione w politykach/systemach bezpieczeństwa w systemach Organizacji.

Zakres dotyczący opisu działań obronnych:

2) Wskazanie działań, mających na celu ograniczenie negatywnego wpływu ataku na środowisko, a co za tym idzie ograniczenie ryzyka

3) Działania manualne możliwe do podjęcia w wypadku danego typu ataku

4) Procedury bezpieczeństwa, np. procedury komunikacji wewnętrznej i informowaniu o zdarzeniu, procedur eskalacji, procedury zarządzania incydentem.

1.1.4. Raport końcowy musi zawierać co najmniej:

1.1.4.1. Dane porządkowe:

a) identyfikator i nazwę scenariusza

b) data utworzenia i zatwierdzenia oraz wersja scenariusza

c) cel i zakres scenariusza

1.1.4.2. Zakres merytoryczny:

a) Opis technik oraz taktyk wskazanych w matrycy MITRE ATT&CK, które powinny zostać uwzględnione w politykach/systemach bezpieczeństwa w systemach organizacji.

b) Wskazanie działań, mających na celu ograniczenie negatywnego wpływu ataku na środowisko, a co za tym idzie ograniczenie ryzyka

c) Działania manualne możliwe do podjęcia w wypadku danego typu ataku

d) Procedury bezpieczeństwa, np. procedury komunikacji wewnętrznej i informowaniu o zdarzeniu, procedur eskalacji, procedury zarządzania incydentem.

1.2. Część nr 2 zamówienia - przedmiotem zamówienia jest świadczenie przez Wykonawcę usługi polegającej na opracowaniu procedury, oceny wpływu norm na proces zabezpieczenia materiału dowodowego oraz skryptów automatyzujących w ramach usługi doradczej z dziedziny digital foresenic (kryminalistyka cyfrowa), w wyniku której Wykonawca opracuje Raport końcowy.

W ramach usługi Wykonawca:

1.2.1. Przygotuje procedurę zabezpieczania i analizy materiału dowodowego w procesie obsługi incydentu bezpieczeństwa z uwzględnieniem „cloud forensics", w tym w oparciu o rozwiązania security Microsoft Defender (Azure);

1.2.2. Przygotuję analizę konsekwencji zastosowania norm ISO 27037, 27041, 27042 oraz 27043 dla procesu zabezpieczania i analizy materiału dowodowego.

1.2.3. Przygotuje skrypty automatyzujące zbieranie informacji o parametrach systemu operacyjnego (Windows) w procesie kolekcjonowania cyfrowego śladu na różnych płatformach sprzętowych z wykorzystaniem narzędzi Open Source (osquery, Volatility 3, oraz innych) oraz komercyjnych będących w użytkowaniu Zamawiającego (Microsoft, TrendMicro).

1.2.4. Raport końcowy musi zawierać co najmniej.

1.2.4.1. Dane porządkowe:

a) Identyfikator i nazwę scenariusza

b) Datę utworzenia i zatwierdzenia oraz wersję scenariusza

c) Cel i zakres scenariusza

1.3. Zamawiający dopuszcza złożenie przez jednego Wykonawcę oferty na dowolnie wybraną przez siebie część lub części zamówienia.

Rozdział II. Termin wykonania zamówienia

1.5. Zamawiający wymaga realizacji zamówienia w następujących terminach:

1.5.1. Część 1 zamówienia - Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania w terminie 40 Dni Roboczych od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru. Wykonawca przedstawi harmonogram wykonania Umowy terminie do 5 Dni Roboczych od podpisania Umowy.

1.5.2. Część 2 zamówienia - Wykonawca zobowiązany jest do realizacji Usługi i wykonania Raportu końcowego spełniającego wymagania w terminie 40 Dni Roboczych od dnia zawarcia Umowy, przy czym przez wykonanie Raportu końcowego rozumie się dostarczenie Raportu końcowego zaakceptowanego przez Zamawiającego poprzez podpisanie bez zastrzeżeń Protokołu Odbioru Wykonawca przedstawi harmonogram wykonania Umowy terminie do 5 Dni Roboczych od podpisania Umowy.

Rozdział III. Warunki udziału w postępowaniu

1.6. O niniejsze zamówienie mogą ubiegać się Wykonawcy spełniający warunki udziału
w postępowaniu w zakresie zdolności technicznej i zawodowej:

1.6.1. Część 1 zamówienia: Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych usługę polegającą na opracowaniu scenariuszy cyberzagrożeń, planów działania i procedur obsługi zdarzeń o wartości każdej z usług nie mniejszej niż 50 000,00 zł brutto (słownie: pięćdziesiąt tysięcy złotych zero groszy).

1.6.2. Część 2 zamówienia: Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że wykonał w okresie ostatnich trzech lat przed upływem terminu składania ofert, a jeżeli okres prowadzenia działalności jest krótszy - w tym okresie, a w przypadku świadczeń powtarzających się lub ciągłych również wykonywanych co najmniej 4 (cztery) usługi polegające na zaprojektowaniu skryptów automatyzujących (playbooków) oraz obsługę incydentów/pobierania danych z sytemu operacyjnego lub platform Threat Intelligence. Wartości każdej z usług powinny być nie mniejsze niż 50 000,00 zł brutto (słownie: pięćdziesiąt tysięcy złotych zero groszy).

1.6.3. Zamawiający uzna, że Wykonawca spełnia warunek udziału we wskazanym zakresie, jeżeli Wykonawca wykaże, że dysponuje następującymi osobami, które zostaną skierowane przez Wykonawcę do realizacji zamówienia, legitymującymi się odpowiednimi kwalifikacjami zawodowymi, wykształceniem i doświadczeniem umożliwiającymi realizację zamówienia na odpowiednim poziomie jakości, tj. dysponuje:

3.1.3.1. Część 1 zamówienia: Co najmniej 2 (dwiema) osobami, każda z nich posiadająca specjalistyczne kwalifikacje potwierdzone jednym ze wskazanych certyfikatów:

a) MITRE ATT&CK (MAD) – Fundamentals

b) MITRE ATT&CK (MAD) - SOC

c) Audytor Wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji wg ISO/IEC 27001:2013

d) CTHP (eLearnSecurity Threat Hunting Professional)

e) CompTIA CASP+ (CompTIA Advanced Security Practitioner)

3.1.3.2. Część 2 zamówienia: Co najmniej 2 (dwiema) osobami, każda z nich posiadająca specjalistyczne kwalifikacje potwierdzone jednym ze wskazanych certyfikatów:

a) BTL1 (Blue Team Level 1)

b) BTL2 (Blue Team Level 2)

c) eCTHP (eLearnSecurity Threat Hunting Professional)

d) CEH (Certified Ethicat Hacker)

e) OSCP (Offensive Security Certified Professional) lub CEH – (Certified Ethicat Hacker) lub CEH – (Certified Ethicat Hacker – Practical).