**Zakup usług konsultingowych z dziedziny cyberbezpieczeństwa:**

**Przedmiotem zamówienia w Zadaniu 1 jest:**

**Opracowanie w ramach Usługi następujących scenariuszy:**

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 niedostępności łączy Internetowych.

Każdy ze scenariuszy powinien opisywać oraz obrazować w postaci graficznej zarówno wektor ataku jak i taktykę defensywną. Dokumenty powinny opierać się na koncepcji Kill Chain, matrycy Mitre ATT&CK oraz Modelu Diamentowym.

Procedury muszą być uniwersalne (dopuszczalne jest wpisanie narzędzi, które już posiada ARiMR), umożliwiające realizację na różnych systemach (procedury nie mogą być vendor-lock). Każda z procedur powinna zawierać maksymalnie 3 warianty.

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

 Zakres detekcji:

1. Weryfikacja alarmów w systemach cyberbezpieczeństwa pod kątem anomali i korelacji;

Zakres odpowiedzi:

1. Zautomatyzowane reagowanie oparte o analizę ryzyka;
2. Działania manualne i i ich weryfikacja skuteczności;
3. Procedury bezpieczeństwa, np. procedury komunikacji wewnętrznej i informowaniu o zdarzeniu, procedury eskalacji, procedury zarządzania incydentem.

**Przedmiotem zamówienia w Zadaniu 2 jest:**

**Przygotowanie:**

1) Przygotowanie procedury zabezpieczania i analizy materiału dowodowego w procesie obsługi incydentu bezpieczeństwa z uwzględnieniem „cloud forensics”, w tym w oparciu o rozwiązania security Microsoft Defender (Azure);

2) Oceny wpływu norm ISO 27037, 27041, 27042 i 27043 dla procesu zabezpieczania i analizy materiału dowodowego;

3) Przygotowanie sykryptów automatyzujących zbieranie informacji o parametrach systemu operacyjnego (Windows) w procesie kolekcjonowania cyfrowego śladu na różnych platformach sprzętowych z wykorzystaniem narzędzi Open Source (osquery, Volatility 3, oraz innych) oraz komercyjnych będących w użytkowaniu Zamawiającego (Microsoft, TrendMicro). W ramach prowadzonej analizy/testowania Wykonawca zapewni niezbędny sprzęt, w szczególności dyski.