**OPIS PRZEDMIOTU ZAMÓWIENIA,**

**DOKUMENTY DOTYCZĄCE SPEŁNIENIA
WARUNKÓW PRZEZ WYKONAWCĘ**

1. **Opis przedmiotu zamówienia:**

Zadanie 8, Podzadanie 8.5., **,, Zakup scenariusza cyberbezpieczeństwo OZE”** - w ramach projektu ,,Wykwalifikowane kadry dla branży OZE” w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027 w ramach Priorytetu I Umiejętności, Działanie 01.05 Umiejętności w szkolnictwie wyższym.

Termin realizacji:

*Zakup będzie realizowany 2 miesiące od dnia podpisania umowy.*

**Kod CPV 38900000-4**

*1.OPIS SCENARIUSZA*

Scenariusz cyberzagrożeń w infrastrukturze odnawialnych źródeł energii (OZE), w szczególności farm wiatrowych, w oparciu o systemy SCADA, PLC oraz inne komponenty infrastruktury technologii operacyjnej (OT). Symulacja obejmuje monitorowanie, analizę i przeciwdziałanie atakom cybernetycznym w środowiskach OT, mając na celu podniesienie świadomości i kompetencji w zakresie cyberbezpieczeństwa oraz wykrywania incydentów w tego typu systemach.

**1. Zakres tematyczny scenariusza::**

- Przeprowadzenie symulacji cyberataków na systemy OT zarządzające farmą wiatrową.

- Analizę zagrożeń związanych z systemami SCADA i PLC.

- Wdrożenie rekomendacji dotyczących zabezpieczenia infrastruktury.

- Edukację uczestników z zakresu identyfikacji zagrożeń oraz podstawowych działań

defensywnych.

**2. Wymagania:**

*2.1 Symulacja - elementy:*

- Topologia sieci farmy wiatrowej obejmuje: minimum 5 maszyn wirtualnych, z

symulowanymi systemami SCADA, PLC oraz narzędziami SIEM.

- Infrastruktura obejmuje: symulator farmy wiatrowej, sterownik OpenPLC, serwer

SCADA oraz firewall OPNSense.

- Symulowane zdarzenia obejmują: różne rodzaje ataków, w tym przerwania

dostępności, przechwycenie danych, wstrzyknięcie złośliwego kodu, ataki typu

Man-in-the-Middle (MiTM).

*2.2 Scenariusze:*

- Rekonesans sieciowy: Wykorzystanie narzędzi takich jak Nmap oraz Hydra do

skanowania i ataków słownikowych.

- Ataki na system SCADA: Symulacje ataków Modbus TCP, ingerencja w rejestry

sterowników PLC, wyłączanie turbin wiatrowych poprzez wysyłanie komend

sterujących.

- Ataki na sterownik PLC: Wykorzystanie podatności systemu OpenPLC, zdalne

wykonywanie kodu, manipulacja parametrami sterującymi.

*3. Konspekt scenariusza*

**Faza 1: Wprowadzenie (30 minut)**

Przedstawienie infrastruktury typowej farmy wiatrowej oraz wprowadzenie do podstawowych zagrożeń cybernetycznych. Omówienie przykładów znanych ataków na infrastrukturę OZE (np. Vestas, Enercon, Nordex).

**Faza 2: Symulacja (120 minut)**

Uczestnicy monitorują symulowane systemy i reagują na zdarzenia. Symulacje obejmują przynajmniej trzy scenariusze ataków, każdy trwający około 40 minut, w tym:

- Symulacja cyberataku.

- Analiza i wyjaśnienie ataku

- Propozycje mitygacji.

**Faza 3: Podsumowanie (30 minut)**

Omówienie zidentyfikowanych zagrożeń oraz potencjalnych skutków dla infrastruktury. Przedstawienie rekomendacji dotyczących mitygacji zagrożeń oraz zabezpieczeń infrastruktury OT.

*4.Szkolenia dla nauczycieli:*

* w ramach zamówienia wykonawca przeprowadzi szkolenie praktyczne dla kadry dydaktycznej prowadzącej zajęcia z wykorzystaniem scenariusza
* wykonawca zapewni realizację szkolenia w wymiarze 6. godzin dla min. 4 nauczycieli
* szkolenie będzie prowadzone w siedzibie Zamawiającego
* wykonawca zapewni wykwalifikowanego trenera

**5. Techniczne:**

* Kompatybilność z platformą cyberpoligon zamawiającego
* Możliwość wielorazowego użycia/włączenia scenariusza w każdym momencie na platformie zamawiającego bez ingerencji dostawcy
* Dostarczenie obrazów maszyn wirtualnych w formacie QCOW2
* Zautomatyzowanie części symulacji i ataków cybernetycznych z wykorzystaniem agentów platformy zamawiającego.
* Dostarczenie skryptów automatyzujących w formie .xml kompatybilnej z platformą zamawiającego
* Dostarczenie topologii sieciowej i połączeń między maszynami wirtualnymi w formie .xml kompatybilnej z platformą zamawiającego
* Integracja z modułem "akcje" na platformie zamawiającego
* Integracja z modułem "Kategorie oceny" na platformie zamawiającego
* Możliwość wprowadzenia zautomatyzowanych akcji oceniających działania uczestników na dowolnym elemencie infrastruktury scenariusza
* Przeprowadzenie testów wydajności dostarczanego scenariusza na platformie zamawiającego
* Kompatybilność z możliwością importu/eksportu scenariusza na platformie zamawiającego
* Integracja dostarczonego scenariusza z platformą zamawiającego

**Wsparcie techniczne: od dnia podpisania umowy do 30.06.2027**