IZP.272.37.2025

ZAŁ. NR 8 - OPIS PRZEDMIOTU ZAMÓWIENIA DLA CZĘŚCI IV

Część 4: Szkolenie dla kadry zarządzającej i informatyków w zakresie zakupionego systemu ESET XDR

Forma szkolenia: Szkolenie w formie online

1. Szkolenie zostanie przeprowadzone w formie on-line dla jednej grupy szkoleniowej.
2. Jednostką czasową szkolenia jest 1 godzina szkoleniowa (45 minut).
3. Szkolenia odbędzie się w ustalonym dniu roboczym, rozpoczęcie nie wcześniej niż 8.00, zakończenie nie później niż 15:30, w terminie uzgodnionym z Zamawiającym.
4. Szkolenie będzie prowadzone w języku polskim.
5. Szkolenie prowadzone będzie na podstawie zaakceptowanego przez Zamawiającego harmonogramu zawierającego zakres merytoryczny, dostarczonego przez Wykonawcę Zamawiającemu przed podpisaniem umowy.
6. Szkolenie musi być na każdym etapie zgodne z zasadami: równości szans i niedyskryminacji, w tym dostępności dla osób z niepełnosprawnościami oraz równości kobiet i mężczyzn.
7. Usługa szkolenia elektronicznego on-line, świadczona przez usługodawcę, musi być dostępna dla wszystkich, bez względu na ich płeć, wiek, pochodzenie, orientację seksualną, niepełnosprawność czy inne przesłanki dyskryminacji

Liczba szkolonych osób: 5

Minimalne wymagania: Szkolenie w wymiarze min. 6 godzin szkoleniowych w języku polskim

Szkolenie ma uwzględniać co najmniej następujące tematy:

- Omówienie pojęcia Extended Detection & Respond (XDR),
- Architektura produktu ESET INSPECT ON-PREM vs wersja CLOUD
- Wdrożenie serwera ESET INSPECT ON-PREM – forma ćwiczenia/warsztatu,
- Wdrożenie i konfiguracja ESET INSPECT CONNECTOR – forma ćwiczenia/warsztatu,
- Omówienie funkcji ESET INSPECT ON-PREM,
- Generowanie detekcji i ich analiza – forma ćwiczenia/warsztatu,
- Reguły i automatyzacja – forma ćwiczenia/warsztatu,
- Raportowanie, powiadomienia i zarządzanie uprawnieniami,
- Rozwiązywanie problemów.

Osoba szkolona powinna:

- zdobyć wiedzę i umiejętności obsługi narzędzia ESET XDR,
- umieć wykryć zagrożenia typu APT (Advanced Persistent Threat),
- umieć wykrywać unikatowe pliki w sieci,
- umieć monitorować aplikacje,
- potrafić wykonywać analizę powłamaniową,
- potrafić chronić firmę przed ransomware,
- potrafić blokować uruchomienie pliku w sieci.

Po szkoleniu kursant otrzymuje:

1. Zaświadczenie ukończenia szkolenia.
2. Materiały szkoleniowe.

Wymaganie dotyczące Wykonawcy:

1. Wykonawca prowadzi autoryzowany ośrodek szkoleniowy ESET.
2. Osoba prowadząca szkolenie winna posiadać stosowną wiedzę oraz min. 3 letnie doświadczenie w przeprowadzeniu szkoleń ESET.

Termin realizacji:

- do dnia 30.09.2025 r.