WL-IV.272.13.2026 Załącznik nr 5 do swz

Opis Przedmiotu Zamówienia

Przedmiotem zamówienia jest przeprowadzenie szkoleń w zakresie cyberbezpieczeństwa dedykowanych dla administratorów systemów informatycznych oraz kadry zarządzającej Komendy Wojewódzkiej Państwowej Straży Pożarnej w Krakowie w celu podniesienia poziomu wiedzy i umiejętności w zakresie ochrony systemów dziedzinowych, wdrażania i utrzymania polityk bezpieczeństwa informacji oraz zarządzania bezpieczeństwem informacji.

Ogólne wymagania dotyczące wszystkich szkoleń:

- Szkolenia będą prowadzone w języku polskim. Dopuszczalne są podręczniki i materiały ze szkoleń w języku angielskim dla szkoleń autoryzowanych.
- Szkolenia co do zasady nie mogą odbywać się w formie e-learningu. Szkolenia mogą się odbyć w formie zdalnej pod warunkiem, że dostawca udostępni własną platformę wideokonferencyjną, która zapewni stały kontakt z trenerem oraz innymi uczestnikami szkolenia i zapewni dostęp on-line do ćwiczeń, laboratoriów itp.
- Szkolenia mogą odbywać się stacjonarnie w siedzibie Komendy Wojewódzkiej Państwowej Straży Pożarnej w Krakowie lub w centrum szkolenia wyznaczonego przez Wykonawcę w Krakowie.
- Szkolenia będą odbywać się w dni robocze.
- Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego harmonogramu. Terminy tur szkoleń nie mogą się pokrywać.
- Szkolenia prowadzone będą na podstawie zaakceptowanego przez Zamawiającego szczegółowego zakresu merytorycznego szkolenia dostarczonego przez Wykonawcę.
- Uczestnicy szkoleń otrzymują certyfikaty ukończenia danego szkolenia.
- Daty szkolenia zostaną ustalone z wybranym Wykonawcą.

Część 1 zamówienia:

<table>
<tr><td colspan="2">Szkolenia</td></tr>
<tr><td colspan="2">Szkolenie z zakresu cyberbezpieczeństwa dla kadry zarządzającej</td></tr>
<tr><td>Uczestników: 4 osoby</td><td>Uczestników w jednej turze: 2 osoby.
Termin szkolenia jednej tury nie może pokrywać się z terminem szkolenia drugiej tury.</td></tr>
<tr><td>Czas trwania: minimum 2 dni (14h)</td><td>Wymagania dotyczące Trenera Prowadzącego:
Specjalista w dziedzinie bezpieczeństwa informacji i cyberzagrożeń posiadający przynajmniej jeden z certyfikatów: CompTIA (CASP+ , CySA+, Security+), CEH</td></tr>
<tr><td colspan="2">Zakres szkolenia:
1. Informacje o zagrożeniach i technologiach związanych z CyberBezpieczeństwem AI - aspekty CyberBezpieczeństwa od zagrożeń wewnętrznych po zagrożenia w obszarze OT/AI oraz łańcucha dostaw,
2. Poznanie technik ofensywnych i obronnych stosowanych w CyberAtakach - techniki wykorzystywane przez cyberprzestępców:
a. socjotechnika,
b. ataki typu MITM,
c. deep fake AI
d. inne możliwe</td></tr>
</table>

3. Zrozumienie regulacji prawnych i ich wpływu na organizacje - krajowe i unijne regulacje dotyczące CyberBezpieczeństwa, w tym RODO, NIS2 oraz Cybersecurity Act,. 4. Zaawansowane ataki celowane (ang. Advanced Persistent Threat) - przedstawienie etapów modelowego ataku celowanego oraz możliwości przeciwdziałania takim atakom 5. Przygotowanie na zarządzanie kryzysowe i odpowiedzialność w przypadku naruszeń - konsekwencje prawne i finansowe związane z niedostosowaniem się do wymogów CyberBezpieczeństwa, w tym odpowiedzialność kadry zarządzającej za zaniedbania w obszarze bezpieczeństwa informacji.

Część 2 zamówienia:

Auditor wewnętrzny Systemu Zarządzania Bezpieczeństwem Informacji	
Uczestników: 2 osoby (tylko jedna tura szkolenia)	Czas trwania: minimum 3 dni (18h)
Wymagania dotyczące Trenera Prowadzącego: Ekspert systemów zarządzania z minimum dwuletnim doświadczeniem w zakresie Certyfikacji systemów zarządzania jakością z ramienia jednostki certyfikującej systemy wg: • PN-EN ISO/IEC 27001, • PN-EN ISO 22301	
Zakres szkolenia: 1. Zapoznanie ze strukturą i elementami Systemu Zarządzania Bezpieczeństwem Informacji - wymagania normy ISO 27001: ○ Kontekst ○ Odpowiedzialność kierownictwa. ○ Planowanie ○ Wsparcie ○ Działania operacyjne ○ Ocena skuteczności ○ Doskonalenie systemu ○ Przegląd wybranych zabezpieczeń Aneks A 2. Pozyskanie wiedzy i umiejętności w zakresie technik audytu wewnętrznego. ○ Planowanie audytu. ○ Prowadzenie badań audytowych. ○ Identyfikacja niezgodności. ○ Dokumentowanie wyników audytu. ○ Udział w działaniach doskonalących. ○ Współpraca zespołów audytorskich. ○ Audyty zintegrowane. 3. Pozyskanie wiedzy i umiejętności dotyczących identyfikacji niezgodności i obszarów doskonalenia Systemu Zarządzania. Bezpieczeństwem Informacji zgodnie z normą ISO 27001.	

Część 3 zamówienia:

CompTIA Security + (szkolenie autoryzowane)	
Uczestników: 5 osób	Szkolenie podzielone na dwie tury po 2 i 3 osoby. Termin szkolenia jednej tury nie może pokrywać się z terminem szkolenia drugiej tury. Czas trwania min: 5 dni (30 h)
Zakres szkolenia obejmujący przygotowanie do egzaminu CompTIA Exam Code SY0-701 lub aktualnego w dniu składania oferty. Szkolenie musi obejmować specjalistyczna wiedzę, którą określa certyfikat z listy certyfikatów w Rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia	

teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. 2022 poz. 131)
Szkolenie musi odbyć się przed szkoleniem CySA+ .

CompTIA Cybersecurity Analyst (CySA+) - szkolenie autoryzowane

Uczestników: 5 osób	Szkolenie podzielone na dwie tury po 2 i 3 osoby. Termin szkolenia jednej tury nie może pokrywać się z terminem szkolenia drugiej tury Czas trwania min: 5 dni (30 h)

Szkolenie musi obejmować specjalistyczna wiedzę, którą określa certyfikat z listy certyfikatów w Rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. 2022 poz. 131)
Zakres szkolenia obejmujący przygotowanie do egzaminu CompTIA Exam Code CS0-003 lub aktualnego w dniu składania oferty.
Szkolenie musi odbyć się po szkoleniu CompTIA Security +.

CompTIA Network+ (szkolenie autoryzowane)

Uczestników: 1 osoba. Czas trwania min: 5 dni (30 h)

Zakres szkolenia:

1. Architektura sieciowa i model referencyjny OSI
   - Porównywanie i kontrastowanie warstw modelu OSI
   - Konfiguracja sieci SOHO
2. Okablowanie sieci Ethernet
   - Standardy Ethernet
   - Okablowanie oparte na miedzi i światłowodzie
3. Przełączanie w sieciach Ethernetowych
   - Wdrażanie urządzeń sieciowych
   - Interfejsy sieciowe
   - Wdrażanie wspólnych funkcji przełączania Ethernet
4. Rozwiązywanie problemów sieci Ethernet
   - Wyjaśnienie metodologii rozwiązywania problemów sieciowych
   - Rozwiązywanie typowych problemów z łącznością kablową
5. Protokół IPv4
   - Wyjaśnienie schematów adresowania IPv4
   - Routing protokołu IPv4
   - Konfiguracja sieci IP i podsieci
6. Wsparcie dla sieci IPv4 i IPv6
   - Narzędzia do testowania konfiguracji IP
   - Rozwiązywanie problemów sieci IP
   - Wyjaśnienie schematów adresowania IPv6
7. Konfigurowanie i rozwiązywanie problemów z routerami
   - Omówienie koncepcji routingu statycznego
   - Omówienie koncepcji routingu dynamicznego
   - Instalacja i rozwiązywanie problemów z routerami
8. Topologie i typy sieci
   - Architektura przełączania warstwowego
   - Wirtualne sieci LAN
9. Protokoły warstwy transportowej
   - Porównanie protokołów warstwy transportowej
   - Weryfikacja otwartych portów sieciowych
10. Usługi sieciowego
    - Wyjaśnienie zastosowania usług adresowania sieciowego
    - Wyjaśnienie zastosowania usług rozwiązywania nazw
    - Konfiguracja usług DNS

11. Aplikacje sieciowego
    - Przykłady usług sieciowych WWW, plików, drukowania, baz danych, e-mail i głosu
12. Dostępność sieci
    - Usługi zarządzania siecią
    - Zarządzanie zdarzeniami w celu zapewnienia dostępności sieci
    - Użycie metryk wydajności w celu zapewnienia dostępności sieci
13. Bezpieczeństwo sieci
    - Podstawowe pojęcia dotyczące bezpieczeństwa
    - Metody uwierzytelniania
14. Rozwiązywanie problemów w zabezpieczonych sieciach
    - Porównanie urządzeń zwiększających bezpieczeństwo
    - Rozwiązywanie problemów z usługami i problemami zabezpieczeń
15. Rozwiązywanie problemów w sieciach bezprzewodowych
    - Standardy sieci bezprzewodowych
    - Instalacja sieci bezprzewodowych
    - Konfiguracja i rozwiązywanie problemów zabezpieczeń sieci bezprzewodowych
16. Łącza WAN i metody zdalnego dostępu
    - Dostawcy usług WAN
    - Metody zdalnego dostępu
17. Koncepcje bezpieczeństwa organizacyjnego i fizycznego
    - Dokumentacja i polityki organizacyjne
    - Metody fizycznego zabezpieczenia
    - Urządzenia IoT
18. Disaster Recovery i High Availability
    - Wyjaśnienie koncepcji odzyskiwania po awarii
    - Wyjaśnienie koncepcji wysokiej dostępności
19. Techniki zabezpieczania sieci
    - Porównanie typów ataków
    - Zastosowanie technik zabezpieczania sieci
20. Architektura chmury i centrum danych
    - Koncepcja chmury
    - Technologie wirtualizacji i technologie SAN (Storage Area Network)
    - Architektura sieci w centrum danych

Szkolenie umożliwia przygotowanie do egzaminu CompTIA Exam Code N10-009.

Część 4 zamówienia:

Certified Ethical Hacker (autoryzowane szkolenie EC-Council)	
Uczestników: 4 osób	Uczestników w jednej turze: po 2 osoby. Czas trwania min: 5 dni (30 h)
Szkolenie musi obejmować specjalistyczna wiedzę, którą określa certyfikat z listy certyfikatów w Rozporządzeniu Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. 2022 poz. 131) Zakres szkolenia obejmujący przygotowanie do egzaminu CEHv13 AI. lub aktualnego w dniu składania oferty.	