Opis przedmiotu zamówienia

Szkolenie z zakresu Bezpieczeństwo systemów Windows i bezpieczeństwo sieci komputerowych

Sekcja 1. Terminologia

1. **Zamawiający** – Katolicki Uniwersytet Lubelski Jana Pawła II
2. **Wykonawca** – instytucja odpowiadająca na zapytanie o cenę zawierające niniejszy OPZ
3. **Certyfikat MCT, MCSE.** Certyfikat wydany przez międzynarodowa instytucję certyfikującą. Opis równoważności znajduję się w sekcji 6.

Sekcja 2. Przedmiot zamówienia

Zamawiający zleci przeszkolenie pracowników Zamawiającego w zakresie:

1) Bezpieczeństwa systemów Windows:

- skuteczne zabezpieczanie systemów Windows przed włamaniami i działaniami "złośliwych" użytkowników,
- wykorzystywanie technik i narzędzi informatycznych w celu podniesienia bezpieczeństwa stacji roboczej z Windows i stworzenia bezpiecznego środowiska do pracy,
- efektywne monitorowanie pracy systemu Windows i wykrywanie anomalii (włamań),
- efektywne lokowanie danych użytkownika ze stacji roboczej do lokalizacji sieciowych,
- poznanie technik ataków charakterystycznych dla środowisk MS Windows,
- poznanie polityk, które pozwolą efektywnie zarządzać i podnosić bezpieczeństwo stacji roboczych z poziomu domeny Windows.

2) Bezpieczeństwa Sieci Komputerowych:

- poznania technik ataków i programów wykorzystywanych współcześnie we włamaniach do sieci,
- sposobów zabezpieczania serwerów i usług przed atakami,
- wykorzystywania narzędzi do testowania bezpieczeństwa sieci,
- przeprowadzania ataków na usługi i urządzenia sieciowe,
- rodzajów i etapów testów penetracyjnych oraz metodyki ich prowadzenia,
- wykonania testu penetracyjnego (analizy ryzyka, identyfikacja podatności, tworzenie raportu)

Szkolenie powinno zawierać również elementy praktyczne.

Wykonawca w ramach zamówienia zapewni dostęp do platformy szkoleniowej, materiały szkoleniowe (podręcznik, zapis z prezentacji) wieczysty dostęp do konta FTP zawierającego dodatkowe, stale aktualizowane materiały dotyczące bezpieczeństwa sieci oraz certyfikat ukończenia szkolenia.

Szkolenie musi być prowadzone w języku polskim.

Sekcja 3. Sprawy organizacyjne

A. Forma i metoda szkolenia

Szkolenie musi być przeprowadzone w formie zdalnej, a trener powinien być dostępny dla uczestników przez cały okres trwania szkolenia.

Wykonawca musi zapewnić narzędzie do komunikacji zdalnej z kursantami. Szkolenie powinno być przeprowadzone w języku polskim.

Materiały udostępniane przez Wykonawcę powinny być w miarę możliwości w języku polskim. Zamawiający dopuszcza możliwość przekazania dokumentów tylko w języku angielskim w razie braku odpowiednika w języku polskim.

Wykonawca zobowiązany będzie do przedstawienia właściwego programu szkolenia w terminie 7 dni, od dnia podpisania umowy z Zamawiającym. Zamawiający zastrzega sobie prawo do wniesienia uwag do właściwego programu szkolenia, w terminie 7 dni od otrzymania go od Wykonawcy. Wykonawca zobowiązany będzie od uwzględnienia uwag Zamawiającego. Wykonawca zobowiązany będzie od uwzględnienia uwag Zamawiającego i przesłania ostatecznego programu w terminie 3 dni.

B. Liczba kursantów

Zamawiający przewiduje przeszkolenie po jednej grupie kursantów z każdego tematu, po 4 osoby na grupę. Łącznie 2 grupy 8 osób.

Zamawiający na 7 dni przed rozpoczęciem szkolenia przekaże Wykonawcy listę uczestników.

C. Termin i czas trwania

Czas szkolenia:

- Grupa nr 1: szkolenie pn. Bezpieczeństwo systemów Windows: 14 godzin zegarowych (tj. 2 dni x 7h)
- Grupa nr 2: szkolenie pn. Bezpieczeństwo sieci komputerowych: 21 godzin zegarowych (tj. 3 dni x 7h)

Szkolenia muszą być przeprowadzone w terminie nie przekraczalnym do 10.12.2023 roku.

Sekcja 4. Ramowy plan szkolenia

W ramach szkolenia pn. Bezpieczeństwo systemów Windows, Zamawiający oczekuje realizacji tematyki zgodnie z rekomendacjami:

- NIST – National Institute of Standards and Technology,
- STIG – Security Technical Implementation Guides,

- CIS Security Benchmark.

Zamawiający oczekuje wykorzystywania narzędzi i technik informatycznych:

- Active Directory Domain Services,
- Group Policy Object,
- Microsoft Security Compliance Toolkit,
- Local Admin Password Solution,
- Sysinternals Sute,
- Access Control List – ograniczenie dla zwykłego użytkownika do tworzenia plików tylko w profilu,
- Advanced Auditing – ustawienia audytu zdarzeń w systemie,
- Event Viewer – ustawienia, archiwizacja logów,
- Event Forwarding – centralna archiwizacja logów,
- User Rights – uprawnienia użytkownika w systemie,
- Restricted Groups – zarządzanie przynależnością do grup lokalnych,
- Security Options – opcje bezpieczeństwa systemu,
- Local Admin Password Solution – zarządzanie wbudowanymi kontami administracyjnymi,
- Services – usługi systemowe,
- AppLocker/SRP – ograniczenie uruchamianych aplikacji tylko do autoryzowanych,
- Integrity Levels – zarządzanie uprawnieniami na obiektach systemowych,
- Firewall & IPSec – systemowa zapora sieciowa,
- Preferences – specyficzne zmiany w rejestrach, np. konfiguracja Adobe Reader, Java,
- Folder Redirection – przekierowywanie folderów użytkownika,
- Internet Explorer 11/Edge,
- Office 2013/2016/2019/2021,
- Enhanced Mitigation Experience Toolkit 5.52/ Windows Defender Exploit Guard,
- Windows Defender Security Center,
- BitLocker – szyfrowanie dysków,
- Microsoft Security Compliance Toolkit – zbiór rekomendowanych ustawień dla produktów Microsoft,
- Sysinternal Suite – pakiet przydatnych narzędzi np. AccessChk, Procmon,
- System Microsoft Windows – konfiguracja środowiska,
- Sysmon,
- File Screening – zarządzanie zawartością na serwerze plików,
- Dynamic Access Control – nowe podejście do nadawania uprawnień.

W ramach szkolenia pn. Bezpieczeństwo sieci komputerowych, Zamawiający oczekuje realizacji tematyki:

- metodyki i rodzaje testów penetracyjnych,
- OSSTMM / OWASP,
- dokumenty opisujące dobre praktyki (NIST/CIS),
- różnice pomiędzy pentestami, a audytami,
- prawne aspekty prowadzenia testów penetracyjnch,
- opracowywanie planu testów penetracyjnych,
- typowy problemy spotykane podczas testów penetracyjnych,
- pasywne metody zbierania informacji o celu,
- wykorzystanie serwerów proxy,

- zbieranie i analiza metadanych,
- ataki typu social-engineering i APT,
- profilowanie pracowników,
- aktywne metody zbierania informacji o celu,
- mapowanie sieci ofiary,
- omijanie firewalli,
- rodzaje podatności (buffer overflow, format string, etc.),
- omówienie shellcode,
- mechanizmy DEP/ASLR i ich omijanie,
- ROP i heap spray'ing,
- dopasowywanie kodu exploita do znalezionych podatności,
- rodzaje exploitów,
- wyszukiwanie exploitów,
- analiza przykładowego exploita,
- tworzenie własnego exploita,
- wybór drogi wejścia do systemu,
- przegląd technik ataków na systemy (Windows/Linux) i sieci komputerowe,
- ataki w sieci LAN/WAN/Wi-Fi,
- ataki na urządzenia sieciowe (routery, switche, IDS/IPS/WAF, firewalle, load balancery),
- ataki denial of service,
- fuzzing,
- łamanie haseł,
- atak przy pomocy exploita zdalnego,
- narzędzia wspomagające atak,
- podniesienie uprawnień do poziomu administratora,
- exploity lokalne,
- łamanie hashy haseł,
- „backdoorowanie" przejętego systemu,
- zacieranie śladów włamania, oszukiwanie narzędzi do analizy powłamaniowej,
- budowa szczegółowego raportu technicznego,
- raport dla zarządu,
- idea honeypotów,
- systemy IDS/IPS,
- metody „hardeningu" systemów operacyjnych,

A. Zaświadczenie uczestnictwa w szkoleniu

Szkolenie musi zakończyć się wydaniem certyfikatu o ukończenia szkolenia.

Sekcja 5: Opis i kryteria równoważności:

Przez certyfikat równoważny do Certyfikatu MCT, MCSE, Zamawiający rozumie certyfikat, który spełnia następujące kryteria:

(a) dziedzina merytoryczna dotycząca bezpieczeństwa systemów informatycznych w organizacji - wynikająca z roli, której dotyczy certyfikat;

(b) przynajmniej podstawowy stopień poziomu kompetencji dla tej dziedziny;

(c) potwierdza poziom kompetencji i umiejętności wymaganego do otrzymania danego certyfikatu;

(d) potwierdzony jest egzaminem przeprowadzonym przez akredytowaną jednostkę certyfikującą.

Sekcja 6: Wykonawca zobowiązuje się do:

- przeprowadzenia szkolenia, zgodnie z planem i harmonogramem przedstawionym przez Zamawiającego. Zamawiający zastrzega, że zajęcia realizowane będą w terminach dogodnych dla uczestników projektu,
- przeprowadzenia szkolenia w taki sposób, by ich poziom i stopień zaawansowania był dostosowany do poziomu grupy,
- zapewnienia materiałów szkoleniowych,
- prowadzenia dokumentacji szkoleniowej na wzorach przekazanych przez Zamawiającego, tj. dzienników zajęć, list obecności, dokumentów potwierdzających przekazanie materiałów szkoleniowych, innych dokumentów przekazanych przez Zamawiającego,

Sekcja 7: Cena szkolenia

Zamawiający oświadcza że usługa zostanie sfinansowana w całości ze środków publicznych w związku z powyższym wykonawca wystawi fakturę bez doliczania do ceny podatku VAT (pozycje zwolnienie VAT) na podstawie art. 43 ust. 1 pkt 29 lit. c ustawy z dnia 11 marca 2004 r. o podatku od towarów i usług(t.j. Dz. U. z 2023 r. poz. 1852 z późn. zm.).